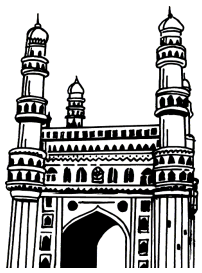
*Rahul's* ✔
*Topper's Voice*

AS PER
CBCS SYLLABUS



# M.C.A

## II Year III Sem

**Latest 2023 Edition**

# INFORMATION SECURITY

- ☞ **Study Manual**
- ☞ **Solved Model Papers**

**- by -**

**WELL EXPERIENCED LECTURER**

₹.199/-

*Rahul Publications*™
**Hyderabad. Cell : 9391018098, 9505799122.**

# M.C.A

## II Year III Sem

# INFORMATION SECURITY

*Inspite of many efforts taken to present this book without errors, some errors might have crept in. Therefore we do not take any legal responsibility for such errors and omissions. However, if they are brought to our notice, they will be corrected in the next edition.*



***Price*** ` : ***199-00***

***Sole Distributors :*** **Cell : 9391018098, 9505799122**

VASU BOOK CENTRE

**Shop No. 2, Beside Gokul Chat, Koti, Hyderabad.**

**Maternity Hospital Opp. Lane, Narayan Naik Complex, Koti, Hyderabad.**
**Near Andhra Bank, Subway, Sultan Bazar, Koti, Hyderabad -195.**

# INFORMATION SECURITY

CONTENTS

## STUDY MANUAL



## SOLVED MODEL PAPERS

# SYLLABUS

## UNIT - I

**Introduction:** History, Critical characteristics of information, NSTISSC security model, Components of an information system, Securing the components, Balancing security and access, The SDLC, The security SDLC. Need for Security: Business needs, Threats, Attacks-secure software development.

## UNIT - II

**Legal, Ethical and professional Issues:** Law and ethics in information security, Relevant U.S lawsinternational laws and legal bodies, Ethics and information security.

**Risk Management:** Overview, Risk identification, Risk assessment, Risk control strategies, selecting a risk control strategy, Quantitive versus qualitative risk control practices, Risk management discussion points, Recommended risk control practices.

## UNIT - III

**Planning for Security:** Security policy, Standards and practices, Security blue print, Security education, Continuity strategies.

**Security Technology:** Firewalls and VPNs, Physical design, Firewalls, Protecting remote connections

## UNIT - IV

**Security Technology:** Intrusion detection, access control and other security. Tolls: Intrusion detection and prevention systems, Scanning and analysis tools, Access control devices.

**Cryptography:** Foundations of cryptology, Cipher methods, Cryptographic Algorithms, Cryptographic tools, Protocols for secure communications, Attacks on cryptosystems.

## UNIT - V

**Implementing Information Security:** Information security project management, Technical topics of implementation, Non technical aspects of implementation, Security certification and accreditation.

**Security and Personnel:** Positioning and staffing security function,Employment policies and practices, Internal control strategies. Information Security maintenance : Security management models, The maintenance model, Digital forensics.

# Contents

**UNIT - V**

UNIT I

**Introduction:** History, Critical characteristics of information, NSTISSC security model, Components of an information system, Securing the components, Balancing security and access, The SDLC, The security SDLC. Need for Security: Business needs, Threats, Attacks- secure software development.

## 1.1 History of Information

**Q1. Explain in brief the history of Information Security.**

*Ans :*

### Introduction

James Anderson, executive consultant at Emagined Security, Inc., believes information security in an enterprise is a well-informed sense of assurance that the information risks and controls are in balance. He is not alone in his perspective. Many information security practitioners recognize that aligning information security needs with business objectives must be the top priority.

### The History of Information Security

The history of information security begins with computer security. The need for computer security—that is, the need to secure physical locations, hardware, and software from threats arose during World War II when the first mainframes, developed to aid computations for communication code breaking, were put to use. Multiple levels of security were implemented to protect these mainframes and maintain the integrity of their data. Access to sensitive military locations, for example, was controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards. The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards.

During these early years, information security was a straight forward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage. One of the first documented security problems that fell outside these categories occurred in the early 1960s, when a systems administrator was working on an MOTD (message of the day) file, and another administrator was editing the password file. A software glitch mixed the two files, and the entire password file was printed on every output file.

### The 1960s

During the Cold War, many more mainframes were brought online to accomplish more complex and sophisticated tasks. It became necessary to enable these mainframes to communicate via a less cumbersome process than mailing magnetic tapes between computer centers. In response to this need, the Department of Defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information. Larry Roberts, known as the founder of the Internet, developed the project—which was called ARPANET—from its inception. ARPANET is the predecessor to the Internet.

### The 1970s and 80s

During the next decade, ARPANET became popular and more widely used, and the potential for its misuse grew. In December of 1973, Robert M. Bob Metcalfe, who is credited with the development of Ethernet, one of the most popular networking protocols, identified fundamental problems with ARPANET security. Individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users. Other problems abounded: vulnerability of

password structure and formats; lack of safety procedures for dial-up connections; and nonexistent user identification and authorization to the system.Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to ARPANET. Because of the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET, network security was referred to as network insecurity.

The movement toward security that went beyond protecting physical locations began with a single paper sponsored by the Department of Defense, the Rand Report R-609, which attempted to define the multiple controls and mechanisms necessary for the protection of a multilevel computer system. The document was classified for almost ten years, and is now considered to be the paper that started the study of computer security. The security—or lack there of—of the systems sharing resources inside the Department of Defense was brought to the attention of researchers in the spring and summer of 1967. At that time, systems were being acquired at a rapid rate and securing them was a pressing concern for both the military and defense contractors.

| Date | Documents |
|---|---|
| 1968 | Maurice Wilkes discusses password security in *Time-Sharing Computer Systems.* |
| 1973 | Schell, Downey, and Popek examine the need for additional security in military systems in *"Preliminary Notes on the Design of Secure Military Computer Systems."*[5] |
| 1975 | The Federal Information Processing Standards (FIPS) examines Digital Encryption Standard (DES) in the *Federal Register*. |
| 1978 | Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," discussing the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software.[6] |
| 1979 | Morris and Thompson author "Password Security: A Case History," published in the Communications of the Association for *Computing Machinery* (ACM). The paper examines the history of a design for a password security scheme on a remotely accessed, time-sharing system. |
| 1979 | Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," discussing secure user IDs and secure group IDs, and the problems inherent in the systems. |
| 1984 | Grampp and Morris write "UNIX Operating System Security." In this report, the authors examine four "important handles to computer security": physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security.[7] |
| 1984 | Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the systems administrator or other privileged users ... the naive user has no chance."[8] |

In June of 1967, the Advanced Research Projects Agency formed a task force to study the process of securing classified information systems. The Task Force was assembled in October of 1967 and met regularly to formulate recommendations, which ultimately became the contents of the Rand Report R-609.

The Rand Report R-609 was the first widely recognized published document to identify the role of management and policy issues in computer security. It noted that the wide utilization of networking components in information systems in the military introduced security risks that could not be mitigated by the routine practices then used to secure these systems. This paper signaled a pivotal moment in computer security history—when the scope of computer security expanded significantly from the safety of physical locations and hardware to include the following:

- Securing the data
- Limiting random and unauthorized access to that data
- Involving personnel from multiple levels of the organization in matters pertaining to information security.

### The 1990s

At the close of the twentieth century, networks of computers became more common, as did the need to connect these networks to each other. This gave rise to the Internet, the first global network of networks. The Internet was made available to the general public in the 1990s, having previously been the domain of government, academia, and dedicated industry professionals. The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet-connected local area network (LAN). After the Internet was commercialized, the technology became pervasive, reaching almost every corner of the globe with an expanding array of uses.

Since its inception as a tool for sharing Defense Department information, the Internet has become an interconnection of millions of networks. At first, these connections were based on defacto standards, because industry standards for interconnection of networks did not exist at that time. These defacto standards did little to ensure the security of information though as these precursor technologies were widely adopted and became industry standards, some degree of security was introduced. However, early Internet deployment treated security as a low priority. In fact, many of the problems that plague e-mail on the Internet today are the result of this early lack of security. At that time, when all Internet and e-mail users were (presumably trustworthy) computer scientists, mail server authentication and e-mail encryption did not seem necessary. Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats.

### 2000 to Present

Today, the Internet brings millions of unsecured computer networks into continuous communication with each other. The security of each computer's stored information is now contingent on the level of security of every other computer to which it is connected. Recent years have seen a growing awareness of the need to improve information security, as well as a realization that information security is important to national defense. The growing threat of cyber-attacks has made governments and companies more aware of the need to defend the computer-controlled control systems of utilities and other critical infrastructure. There is also growing concern about nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended.

## 1.2 Critical Characteristics of Information

**Q2. Describe the critical characteristics of information.**

**Or**

**List and explain the critical characteristics of information security?**

*Ans :*

Information Security is a well-informed sense of assurance that the information risk and control are in balance. The protection of information and its critical element includes

**a)** **Availability** - this enables authorized users (either persons or other computer systems) access to information without interference or obstruction & to receive it in the required & or requested format.

**b)** **Accuracy** - the information has to be free from mistakes/errors & has a value that the end user expects-anything that has been modified is no longer an accurate representation of that data.

**c)** **Authenticity** - the quality/state of being genuine or original rather than a reproduction /copy & is considered such when it's in the same state as when it was created, placed, stored or transferred.

**d)** **Confidentiality** - this ensures that only those with the rights & privileges can access that information requested & that the information is protected through a number of measures such as information classification, secure document storage, application of security policies & education of custodians & end users.

**e)** **Integrity** - this is information that is whole, complete & uncorrupted. To prevent this from happening, various methods are used to ensure data integrity such as algorithms, hash values & error-correcting codes. An example can be detecting a virus or a worm by looking for changes in the size of a known file in the operating system or in the computer's documents section.

**f)** **Utility** - this is the quality or state of having value when it can serve a particular purpose or end within the requested format. When it's not a meaningful format, the data is useless to the user.

**g)** **Possession** - this is the state or quality of ownership/control of some object or item (data is said to be in the possession of the one who has obtained it-independent of format or other characteristics.)

**h)** **Confidentiality-** Confidentiality of information ensures that only those with sufficient privileges may access certain information. When unauthorized individuals or systems can access information, confidentiality is breached. To protect the confidentiality of information, a number of measures are used:

- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end users Example, a credit card transaction on the Internet.
- The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in data bases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored.
- Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information, it could result in a breach of confidentiality.

**i)** **Privacy-** The information that is collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected. This definition of privacy does focus on freedom from observation (the meaning usually associated with the word), but rather means that information will be used only in ways known to the person providing it.

**j)** **Identification -** An information system possesses the characteristic of identification when it is able to recognize individual users. Identification and authentication are essential to establishing the level of access or authorization that an individual is granted.

**k)** **Authorization -** After the identity of a user is authenticated, a process called authorization provides assurance that the user (whether a person or a computer) has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset.

**l)** **Accountability-** The characteristic of accountability exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process. For example, audit logs that track user activity on an information system provide accountability.

**NOTE:** Breach of confidentiality always results in the breach of possession but, not always vice versa. Identify the 6 components of an information system. The components of an information system that allow informational data to be inputted, processed, outputted & stored are: software, hardware, data, people, procedures & networks.

**Which are most directly impacted by the study of computer security?**

The ones that are most directly impacted by the study of computer security would be the software programs used by computers, the people that input data to be processed by the computer software programs, the procedures that are used by the people when inputting data into the computer software programs that are used & the network connections that are used by the people that input the data that is processed by the computer software programs in use.

**Which are most commonly associated with this study?**

The ones that are more commonly associated with this field of study would be that of the software programs that are used on the computers, the hardware components that are used on the computers, the data that is inputted into the computers to be processed by the software programs, the people that are using all of the above components for the output of returning data & the procedures that they have to follow for the retrieval of the results of the inputted data.

## 1.3 NSTISSC Security Model

**Q3. What is Information security? Explain the NSTISSC security model and the top-down approach to security implementation.**

*Ans :*

Understanding the technical aspects of information security requires that you know the definitions of certain information technology terms and concepts.

In general, security is defined as the quality or state of being secure—to be free from danger. Security is often achieved by means of several strategies usually undertaken simultaneously or used in combination with one another.

**Specialized areas of security**

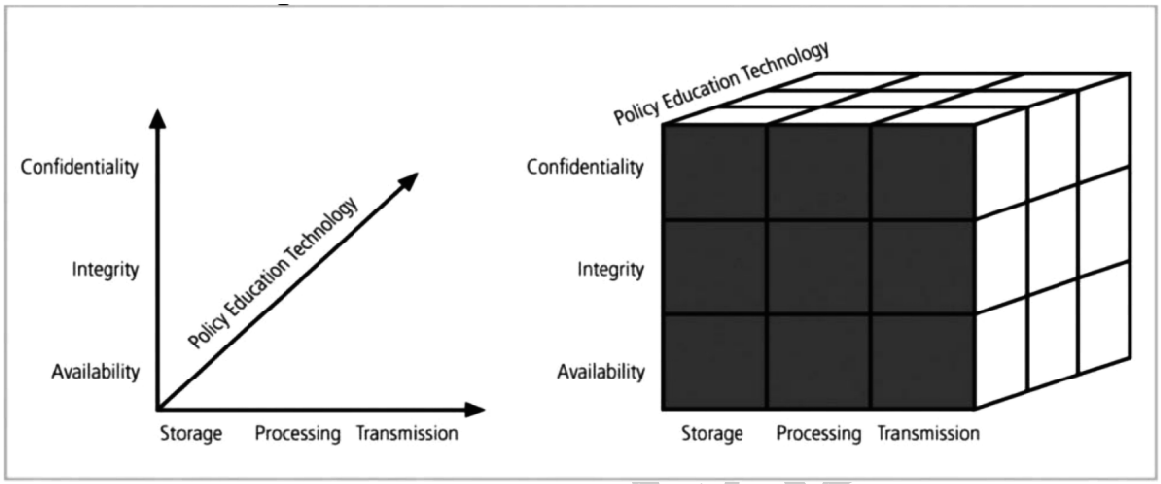
- **Physical security**, which encompasses strategies to protect people, physical assets, and the workplace from various threats including fire, unauthorized access, or natural disasters.
- **Personal security**, which overlaps with physical security in the protection of the people within the organization
- **Operations security**, which focuses on securing the organization's ability to carry out its operational activities without interruption or compromise
- **Communications security**, which encompasses the protection of an organization's communications media, technology, and content, and its ability to use these tools to achieve the organization's objectives
- **Network security**, which addresses the protection of an organization's data networking devices, connections, and contents, and the ability to use that network to accomplish the organization's data communication functions
- **Information security** includes the broad areas of information security management, computer and data security, and network security.

**NSTISSC Security Model (National Security Telecommunications & Information systems security committee' document.)**

- It is now called **the National Training Standard for Information security** professionals.
- The NSTISSC Security Model provides a more detailed perspective on security.
- While the NSTISSC model covers the three dimensions of information security, it omits discussion of detailed guidelines and policies that direct the implementation of controls.
- Another weakness of using this model with too limited an approach is to view it from a single perspective.
- The 3 dimensions of each axis become a 3x3x3 cube with 27 cells representing areas

that must be addressed to secure today's Information systems.

- To ensure system security, each of the 27 cells must be properly addressed during the security process.
- For example, the intersection between technology, Integrity & storage areas requires a control or safeguard that addresses the need to use technology to protect the Integrity of information while in storage.




## 1.4 COMPONENTS OF AN INFORMATION SYSTEM

**Q.4 What Is an Information System? Describe the Components of Information System?**

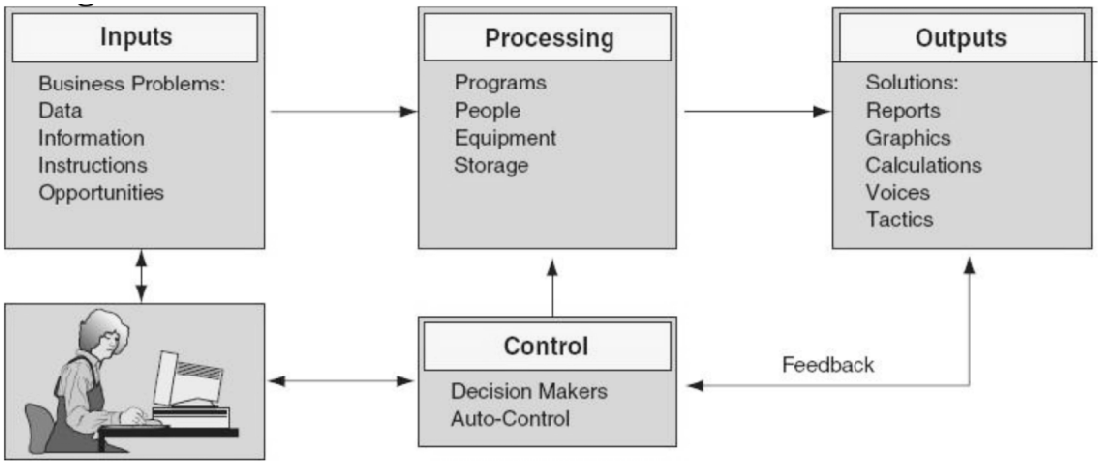
*Ans :*

Information system has been defined in terms of two perspectives: one relating to its function; the other relating to its structure. From a **functional perspective**; an information system is a technologically implemented medium for the purpose of recording, storing, and disseminating linguistic expressions as well as for the supporting of inference making. From a **structural perspective**; an information system consists of a collection of people, processes, data, models, technology and partly formalized language, forming a cohesive structure which serves some organizational purpose or function.

The functional definition has its merits in focusing on what actual users - from a conceptual point of view- do with the information system while using it. They communicate with experts to solve a particular problem. The structural definition makes clear that IS are socio-technical systems, i.e., systems consisting of humans, behavior rules, and conceptual and technical artifacts.

An information system can be defined **technically** as a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision making and control in an organization. In addition to supporting decision making, coordination, and control, information systems may also help managers and workers analyze problems, visualize complex subjects, and create new products.

Three activities in an information system produce the information that organizations need to make decisions, control operations, analyze problems, and create new products or services. These activities are input, processing, and output. Input captures or collects raw data from within the organization or from its external environment. Processing converts this raw input into a more meaningful form. Output transfers the processed information to the people who will use it or to the activities for which it will be used. Information systems also require feedback, which is output that is returned to appropriate members of the organization to help them evaluate or correct the input stage.




**Components of Information Systems**

- **Resources of people:** (end users and IS specialists, system analyst, programmers, data administrators etc.).
- **Hardware:** (Physical computer equipments and associate device, machines and media).
- **Software:** (programs and procedures).
- **Data:** (data and knowledge bases), and Networks: (communications media and network support).

**People Resources**

- **End users:** (also called users or clients) are people who use an information system or the information it produces. They can be accountants, salespersons, engineers, clerks, customers, or managers. Most of us are information system end users.
- **IS Specialists:** people who actually develop and operate information systems. They include systems analysts, programmers, testers, computer operators, and other managerial, technical, and clerical IS personnel. Briefly, systems analysts design information systems based on the information requirements of end uses, programmers prepare computer programs based on the specifications of systems analysts, and computer operators operate large computer systems.

**Hardware Resources**

- **Machines:** as computers and other equipment along with all data media, objects on which data is recorded and saved.
- **Computer systems:** consist of variety of interconnected peripheral devices. Examples are microcomputer systems, midrange computer systems, and large computer systems.

**Software Resources**

Software Resources includes all sets of information processing instructions. This generic concept of software includes not only the programs, which direct and control computers but also the sets of information processing (procedures). Software Resources includes:

- System software, such as an operating system
- Application software, which are programs that direct processing for a particular use of computers by end users.
- Procedures, which are operating instructions for the people, who will use an information system. Examples are instructions for filling out a paper form or using a particular software package.

**Data Resources**

Data resources include data (which is raw material of information systems) and database. Data can take many forms, including traditional alphanumeric data, composed of numbers and alphabetical and other characters that describe business transactions and other events and entities. Text data, consisting of sentences and paragraphs used in written communications; image data, such as graphic shapes and figures; and audio data, the human voice and other sounds, are also important forms of data. Data resources must meet the following criteria:

- **Comprehensiveness:** means that all the data about the subject are actually present in the database.
- **Non-redundancy:** means that each individual piece of data exists only once in the database.
- **Appropriate structure:** means that the data are stored in such a way as to minimize the cost of expected processing and storage.

The data resources of IS are typically organized into:

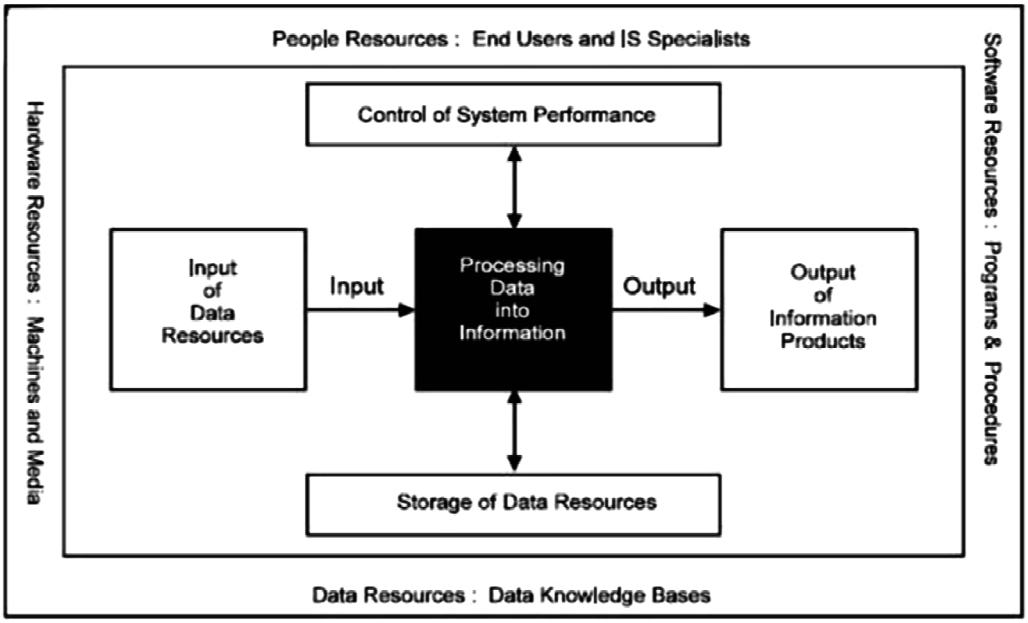
- Processed and organized data-Databases.
- Knowledge in a variety of forms such as facts, rules, and case examples about successful business practices.



**Network Resources**

Telecommunications networks like the Internet, intranets, and extranets have become essential to the successful operations of all types of organizations and their computer-based information systems. Telecommunications networks consist of computers, communications processors, and other devices interconnected by communications media and controlled by communications software. The concept of Network Resources emphasizes that communications networks are a fundamental resource component of all information systems. Network resources include:

- Communications media: such as twisted pair wire, coaxial cable, fiber-optic cable, microwave systems, and communication satellite systems.
- Network support: This generic category includes all of the people, hardware, software, and data resources that directly support the operation and use of a communications network. Examples include communications control software such as network operating systems and Internet packages.




## 1.5 SECURING THE COMPONENTS

**Q5. Explain the 2 functional approaches of information security performed by organization.**

*Ans :*

**Approaches to Information Security Implementation**

The implementation of information security in an organization must begin somewhere, and cannot happen overnight. Securing information assets is in fact an incremental process that requires coordination, time, and patience. Information security can begin as a grassroots effort in which systems administrators attempt to improve the security of their systems. This is often referred to as a **bottom-up approach**. The key advantage of the bottom-up approach is the technical expertise of the individual administrators. Working with information systems on a dayto-day basis, these administrators possess in-depth knowledge that can greatly enhance the development of an information security system. They know and understand the threats to their systems and the mechanisms needed to protect them successfully. Unfortunately, this approach seldom works, as it lacks a number of critical features, such as participant support and organizational staying power.

The **top-down approach**—in which the project is initiated by upper-level managers who issue policy, procedures and processes, dictate the goals and expected outcomes, and determine accountability for each required action—has a higher probability of success. This approach has strong upper-management support, a dedicated champion, usually dedicated funding, a clear planning and implementation process, and the means of influencing organizational culture. The most successful kind of top-down approach also involves a formal development strategy referred to as a systems development life cycle.

For any organization-wide effort to succeed, management must buy into and fully support it. The role played in this effort by the champion cannot be overstated. Typically, this champion is an executive, such as a chief information officer (CIO) or the vice president of information technology (VP-IT), who moves the project forward, ensures that it is properly managed, and pushes for acceptance throughout

the organization. Without this high-level support, many midlevel administrators fail tomake time for the project or dismiss it as a low priority. Also critical to the success of this type of project is the involvement and support of the end users. These individuals are most directly affected by the process and outcome of the project and must be included in the information security process. Key end users should be assigned to a developmental team, known as the joint application development team (JAD). To succeed, the JAD must have staying power. It must be able to survive employee turnover and should not be vulnerable to changes in the personnel team that is developing the information security system. This means the processes and procedures must be documented and integrated into the organizational culture. They must be adopted and promoted by the organization's management.

## 1.6 Balancing Security and Access

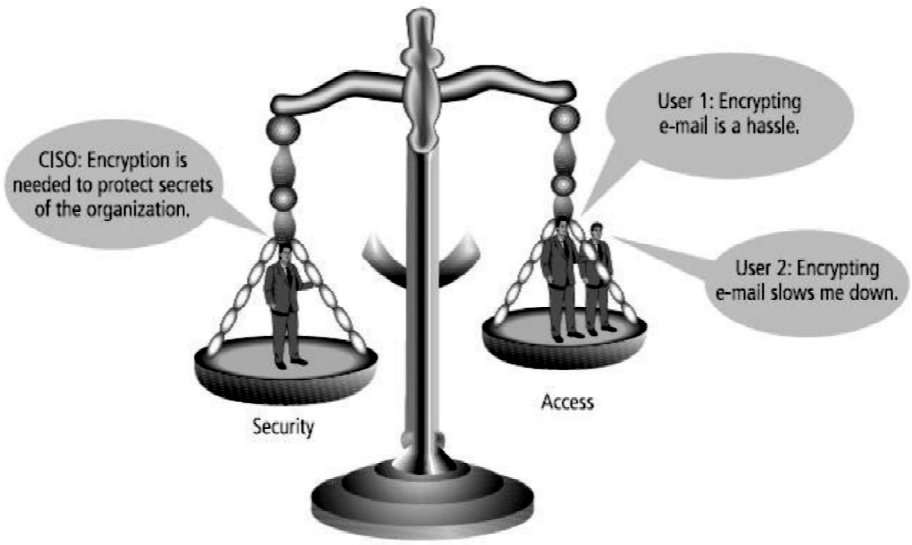
**Q6. Explain the best planning & implementation of Information Security.**

*Ans :*

Even with the best planning and implementation, it is impossible to obtain perfect information security. Recall James Anderson's statement from the beginning which emphasizes the need to balance security and access. Information security cannot be absolute: it is a process, not a goal. It is possible to make a system available to anyone, anywhere, anytime, through any means. However, such unrestricted access poses a danger to the security of the information. On the other hand, a completely secure information system would not allow anyone access. For instance, when challenged to achieve a TCSEC C-2 level security certification for its Windows operating system, Microsoft had to remove all networking components and operate the computer from only the console in a secured room.

To achieve balance—that is, to operate an information system that satisfies the user and the security professional—the security level must allow reasonable access, yet protect against threats.

Because of today's security concerns and issues, an information system or data-processing department can get too entrenched in the management and protection of systems. An imbalance can occur when the needs of the end user are undermined by too heavy a focus on protecting and administering the information systems. Both information security technologists and end users must recognize that both groups share the same overall goals of the organization—to ensure the data is available when, where, and how it is needed, with minimal delays or obstacles. In an ideal world, this level of availability can be met even after concerns about loss, damage, interception, or destruction have been addressed.



## 1.7 THE SDLC

**Q7. Explain different stages of development in SDLC.**

*Ans :*

Many system development life cycle (SDLC) models exist that can be used by an organization to effectively develop an information system. Security should be incorporated into all phases, from initiation to disposition, of an SDLC model. This Bulletin lays out a general SDLC that includes five phases. Each of the five phases includes a minimum set of information security tasks needed to effectively incorporate security into a system during its development.

**Software Development Methodologies**

The most frequently used software development models include:

- **Waterfall:** This technique applies a traditional approach to software development. Groups across different disciplines and units complete an entire phase of the project before moving on to the next step or the next phase. As a result, business results are delivered at a single stage rather than in an iterative framework.
- **Agile:** Adaptive planning, evolutionary development, fast delivery, continuous improvement, and a highly rapid and flexible response to external factors are all key components of an Agile approach. Developers rely on a highly collaborative, crossfunctional framework — with a clear set of principles and objectives — to speed development processes.
- **Lean Software Development (LSD):** This methodology relies on techniques and practices used within a lean manufacturing environment to establish a more efficient and fast development culture. These techniques and practices include eliminating waste, amplifying learning, making decisions as late in the process as possible, delivering fast, empowering a team, embracing integrity, and viewing development as broadly as possible.
- **DevOps:** This technique combines "development" and "operations" functions in order to build a framework focused on collaboration and communication. It aims to automate processes and introduce an environment focused on continuous development. Learn how CA Veracode enables DevOps.
- **Iterative Development:** As the name implies, iterative software development focuses on an incremental approach to coding. The approach revolves around shorter development cycles that typically tackle smaller pieces of development. It also incorporates repeated cycles: an initialization step, an iteration step, and a project control list. Iterative development is typically used for large projects.
- **Spiral Development**: This framework incorporates different models, based on what works best in a given development process or situation. As a result, it may rely on waterfall, Agile, or DevOps for different components or for different projects that fit under the same software development initiative. Spiral uses a risk-based analysis approach to identify the best choice for a given situation.
- **V-Model Development:** The approach is considered an extension of waterfall development methodologies. It revolves around testing methods and uses a V-shaped model that focuses on verification and validation.

**SDLC Phases**

A typical SDLC has six phases:

- Requirements Analysis
- Architecture and Design
- Development
- Testing
- Deployment/Implementation
- Operations/Maintenance

From a security perspective, each phase has its own set of tasks that need to be accomplished to infuse the appropriate level of security into the final system. Each phase and its set of tasks is discussed

in turn. For each, we define the phase, explain in general term s what we are trying to accomplish from a security perspective, and discuss key securityrelated tasks.

We won't get into the many non-security-related tasks that application developers face; we focus on security alone. We discuss the relatively more important tasks, and ones that need further elaboration. Appendix A includes a more comprehensive list of security-related tasks. The method upon which it is based.

- **Methodology and Phases**

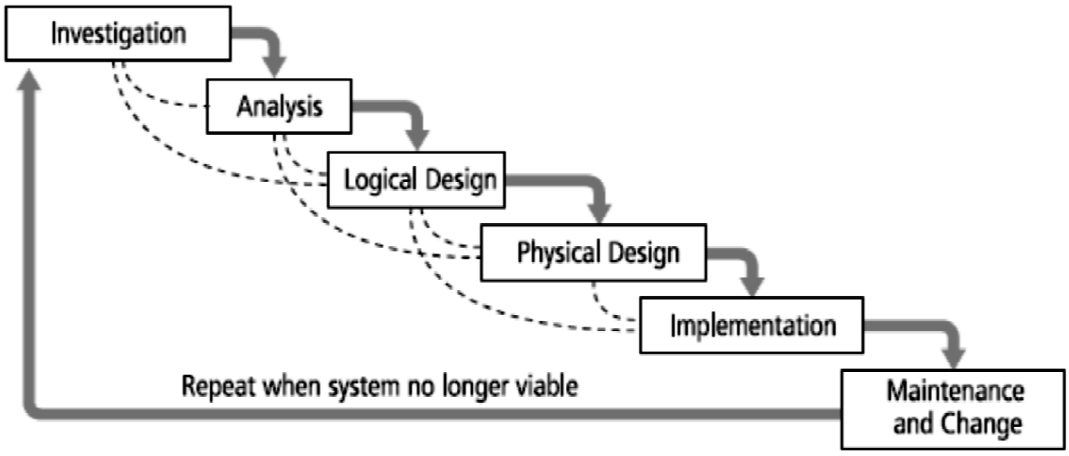
The **systems development life cycle (SDLC)** is a methodology for the design and implementation of an information system. A **methodology** is a formal approach to solving a problem by means of a structured sequence of procedures. Using a methodology ensures a rigorous process with a clearly defined goal and increases the probability of success. Once a methodology has been adopted, the key milestones are established and a team of individuals is selected and made accountable for accomplishing the project goals.

The traditional SDLC consists of six general phases. If you have taken a system analysis and design course, you may have been exposed to a model consisting of a different number of phases. SDLC models range from having three to twelve phases, all of which have been mapped into the six presented here. The **waterfall model** picture illustrates that each phase begins with the results and information gained from the previous phase.

At the end of each phase comes a structured review or reality check, during which the team determines if the project should be continued, discontinued, outsourced, postponed, or returned to an earlier phase depending on whether the project is proceeding as expected and on the need for additional expertise, organizational knowledge, or other resources.

Once the system is implemented, it is maintained (and modified) over the remainder of its operational life. Any information systems implementation may have multiple iterations as the cycle is repeated over time. Only by means of constant examination and renewal can any system, especially an information security program, perform up to expectations in the constantly changing environment in which it is placed.

The following sections describe each phase of the traditional SDLC.




- **Investigation**

The first phase, investigation, is the most important. What problem is the system being developed to solve? The investigation phase begins with an examination of the event or plan that initiates the process. During the investigation phase, the objectives, constraints, and scope of the project are

specified. A preliminary cost-benefit analysis evaluates the perceived benefits and the appropriate levels of cost for those benefits. At the conclusion of this phase, and at every phase following, a feasibility analysis assesses the economic, technical, and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

- **Analysis**

The analysis phase begins with the information gained during the investigation phase. This phase consists primarily of assessments of the organization, its current systems, and its capability to support the proposed systems. Analysts begin by determining what the new system is expected to do and how it will interact with existing systems. This phase ends with the documentation of the findings and an update of the feasibility analysis.

- **Logical Design**

In the logical design phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem. In any systems solution, it is imperative that the first and driving factor is the business need. Based on the business need, applications are selected to provide needed services, and then data support and structures capable of providing the needed inputs are chosen. Finally, based on all of the above, specific technologies to implement the physical solution are delineated. The logical design is, therefore, the blueprint for the desired solution. The logical design is implementation independent, meaning that it contains no reference to specific technologies, vendors, or products. It addresses, instead, how the proposed system will solve the problem at hand. In this stage, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits, allowing for a general comparison of available options. At the end of this phase, another feasibility analysis is performed.

- **Physical Design**

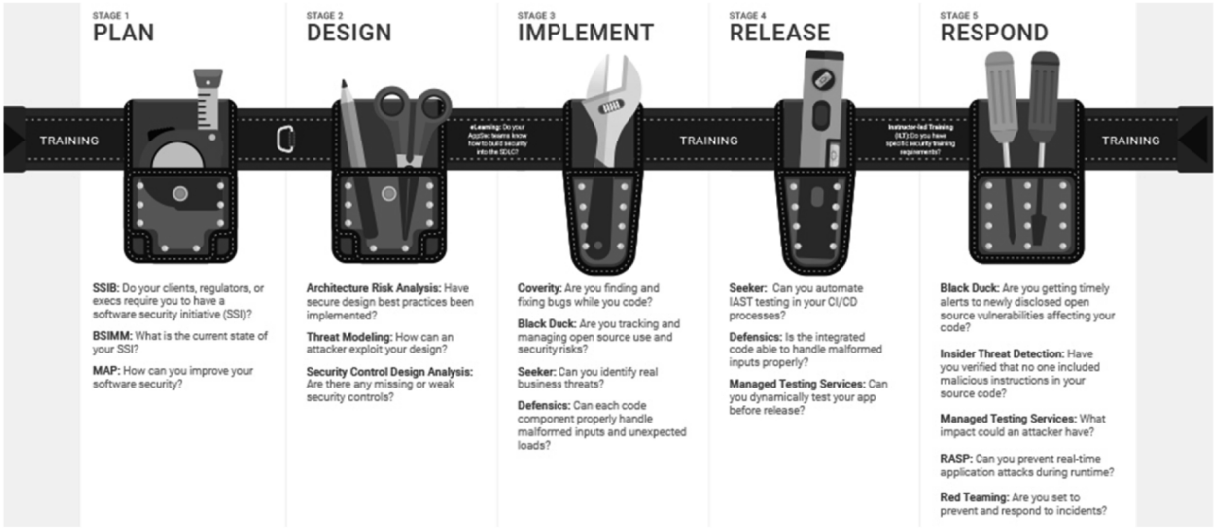
During the physical design phase, specific technologies are selected to support the alternatives identified and evaluated in the logical design. The selected components are evaluated based on a make-or-buy decision (develop the components in-house or purchase them from a vendor). Final designs integrate various components and technologies. After yet another feasibility analysis, the entire solution is presented to the organizational management for approval.

- **Implementation**

In the implementation phase, any needed software is created. Components are ordered, received, and tested. Afterward, users are trained and supporting documentation created. Once all components are tested individually, they are installed and tested as a system. Again a feasibility analysis is prepared, and the sponsors are then presented with the system for a performance review and acceptance test.

- **Maintenance and Change**

The maintenance and change phase is the longest and most expensive phase of the process. This phase consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle. Even though formal development may conclude during this phase, the life cycle of the project continues until it is determined that the process should begin again from the investigation phase. At periodic points, the system is tested for compliance, and the feasibility of continuance versus discontinuance is evaluated. Upgrades, updates, and patches are managed. As the needs of the organization change, the systems that support the organization must also change. It is imperative that those who manage the systems, as well as those who support them, continually monitor the effectiveness of the systems in relation to the organization's environment. When a current system can no longer support the evolving mission of the organization, the project is terminated and a new project is implemented.




Each of the example SDLC phases [discussed earlier] includes a minimum set of security steps needed to effectively incorporate security into a system during its development. An organization will either use the general SDLC described [earlier] or will have developed a tailored SDLC that meets their specific needs. In either case, NIST recommends that organizations incorporate the associated IT security steps of this general SDLC into their development process:

**Investigation/Analysis Phases**

- **Security categorization**—defines three levels (i.e., low, moderate, or high) of potential impact on organizations or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). Security categorization standards assist organizations in making the appropriate selection of security controls for their information systems.
- **Preliminary risk assessment**—results in an initial description of the basic security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.

**Logical/Physical Design Phases**

- **Risk assessment**—analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific.
- **Security functional requirements analysis**—analysis of requirements that may include the following components:
  - system security environment (i.e., enterprise information security policy and enterprise security architecture)
  - security functional requirements
- **Security assurance requirements analysis**—analysis of requirements that address the developmental activities required and assurance evidence needed to produce the desired level of confidence that the information security will work correctly and effectively. The analysis, based on legal and functional security requirements, will be used as the basis for determining how much and what kinds of assurance are required.

- **Cost considerations and reporting**—determines how much of the development cost can be attributed to information security over the life cycle of the system. These costs include hardware, software, personnel, and training.
- **Security planning**—ensures that agreed upon security controls, planned or in place, are fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/ accreditations, and plan of action and milestones).
- **Security control development**—ensures that security controls described in the respective security plans are designed, developed, and implemented. For information systems currently in operation, the security plans for those systems may call for the development of additional security controls to supplement the controls already in place or the modification of selected controls that are deemed to be less than effective.
- **Developmental security test and evaluation**—ensures that security controls developed for a new information system are working properly and are effective. Some types of security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until the information system is deployed—these controls are typically management and operational controls.
- **Other planning components**—ensures that all necessary components of the development process are considered when incorporating security into the life cycle. These components include selection of the appropriate contract type, participation by all necessary functional groups within an organization, participation by the certifier and accreditor, and development and execution of necessary contracting plans and processes.

**Implementation Phase**

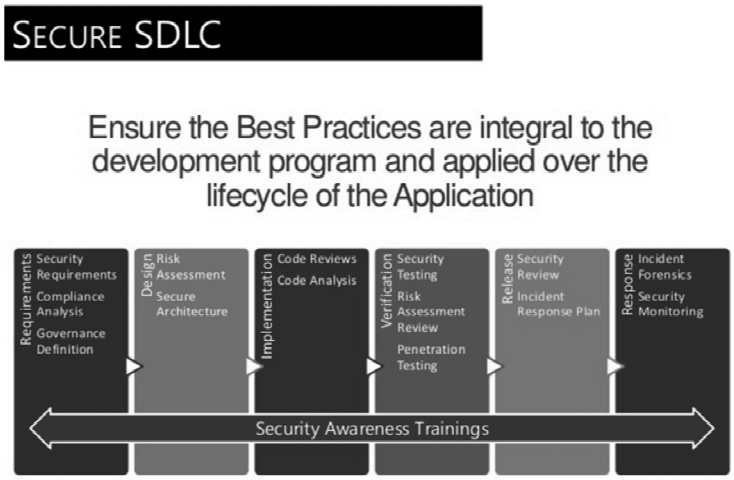
- **Inspection and acceptance**—ensures that the organization validates and verifies that the functionality described in the specification is included in the deliverables. System integration—ensures that the system is integrated at the operational site where the information system is to be deployed for operation. Security control settings and switches are enabled in accordance with vendor instructions and available security implementation guidance.
- **Security certification**—ensures that the controls are effectively implemented through established verification techniques and procedures and gives organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information system. Security certification also uncovers and describes the known vulnerabilities in the information system.
- **Security accreditation**—provides the necessary security authorization of an information system to process, store, or transmit information that is required. This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.

**Maintenance and Change Phase**

- **Configuration management and control**—ensures adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software, and firmware

components for the information system and subsequently controlling and maintaining an accurate inventory of any changes to the system.

- **Continuous monitoring**—ensures that controls continue to be effective in their application through periodic testing and evaluation. Security control monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the security status of the information system to appropriate agency officials is an essential activity of a comprehensive information security program.
- **Information preservation**—ensures that information is retained, as necessary, to conform to current legal requirements and to accommodate future technology changes that may render the retrieval method obsolete.
- **Media sanitization**—ensures that data is deleted, erased, and written over as necessary.
- **Hardware and software disposal**—ensures that hardware and software is disposed of as directed by the information system security officer. Adapted from Security Considerations in the Information System Development Life Cycle.




## 1.8 THE SECURITY SDLC

**Q8. What are the different stages of security SDLC in detail?**

*Ans :*

Each of the example SDLC phases [discussed earlier] includes a minimum set of security steps needed to effectively incorporate security into a system during its development. An organization will either use the general SDLC described [earlier] or will have developed a tailored SDLC that meets their specific needs. In either case, NIST recommends that organizations incorporate the associated IT security steps of this general SDLC into their development process:

**Analysis**

In the analysis phase, the documents from the investigation phase are studied. The development team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls. This phase also includes an analysis of relevant legal issues that

could affect the design of the security solution. Increasingly, privacy laws have become a major consideration when making decisions about information systems that manage personal information. Recently, many states have implemented legislation making certain computer-related activities illegal. A detailed understanding of these issues is vital. Risk management also begins in this stage.

- **Risk management** is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information stored and processed by the organization.

- **Logical Design**

  The logical design phase creates and develops the blueprints for information security, and examines and implements key policies that influence later decisions. Also at this stage, the team plans the incident response actions to be taken in the event of partial or catastrophic loss. The planning answers the following questions:

  - **Continuity planning:** How will business continue in the event of a loss?
  - **Incident response:** What steps are taken when an attack occurs?
  - **Disaster recovery:** What must be done to recover information and vital systems immediately after a disastrous event?

  Next, a feasibility analysis determines whether or not the project should be continued or be outsourced.

- **Physical Design**

  The physical design phase evaluates the information security technology needed to support the blueprint outlined in the logical design generates alternative solutions, and determines a final design. The information security blueprint may be revisited to keep it in line with the changes needed when the physical design is completed. Criteria for determining the definition of successful solutions are also prepared during this phase. Included at this time are the designs for physical security measures to support the proposed technological solutions. At the end of this phase, a feasibility study determines the readiness of the organization for the proposed project, and then the champion and sponsors are presented with the design. At this time, all parties involved have a chance to approve the project before implementation begins.

- **Implementation**

  The implementation phase in of SecSDLC is also similar to that of the traditional SDLC. The security solutions are acquired (made or bought), tested, implemented, and tested again. Personnel issues are evaluated, and specific training and education programs conducted. Finally, the entire tested package is presented to upper management for final approval.

- **Maintenance and Change**

  Maintenance and change is the last, though perhaps most important, phase, given the current ever-changing threat environment. Today's information security systems need constant monitoring, testing, modification, updating, and repairing. Applications systems developed within the framework of the traditional SDLC are not designed to anticipate a software attack that requires some degree of application reconstruction. In information security, the battle for stable, reliable systems is a defensive one. Often, repairing damage and restoring information is a constant effort against an unseen adversary. As new threats emerge and old threats evolve, the information security profile of an organization must constantly adapt to prevent threats from successfully penetrating sensitive data. This constant vigilance and security can be compared to that of a fortress where threats from outside as well as from within must be constantly monitored and checked with continuously new and more innovative technologies.

## Need For Security

### 1.9 Business Needs

**Q9. What are the 3 components C.I.A traingle? What are they used for? Why is it so commonly use in security?**

*Ans :*

| Phases | Steps common to both the systems development life cycle and the security systems development life cycle | Steps unique to the security systems development life cycle |
|---|---|---|
| Phase 1: Investigation | • Outline project scope and goals<br>• Estimate costs<br>• Evaluate existing resources<br>• Analyze feasibility | • Management defines project processes and goals and documents these in the program security policy |
| Phase 2: Analysis | • Assess current system against plan developed in Phase 1<br>• Develop preliminary system requirements<br>• Study integration of new system with existing system<br>• Document findings and update feasibility analysis | • Analyze existing security policies and programs<br>• Analyze current threats and controls<br>• Examine legal issues<br>• Perform risk analysis |
| Phase 3: Logical Design | • Assess current business needs against plan developed in Phase 2<br>• Select applications, data support, and structures<br>• Generate multiple solutions for consideration<br>• Document findings and update feasibility analysis | • Develop security blueprint<br>• Plan incident response actions<br>• Plan business response to disaster<br>• Determine feasibility of continuing and/or outsourcing the project |
| Phase 4: Physical Design | • Select technologies to support solutions developed in Phase 3<br>• Select the best solution<br>• Decide to make or buy components<br>• Document findings and update feasibility analysis | • Select technologies needed to support security blueprint<br>• Develop definition of successful solution<br>• Design physical security measures to support techno logical solutions<br>• Review and approve project |
| Phase 5: Implementation | • Develop or buy software<br>• Order components<br>• Document the system<br>• Train users<br>• Update feasibility analysis<br>• Present system to users<br>• Test system and review performance | • Buy or develop security solutions<br>• At end of phase, present tested package to management for approval |
| Phase 6: Maintenance and Change | • Support and modify system during its useful life<br>• Test periodically for compliance with business needs<br>• Upgrade and patch as necessary | • Constantly monitor, test, modify, update, and repair to meet changing threats |

Information security performs four important functions for an organization:

(1) Protects the organization's ability to function

(2) Enables the safe operation of applications implemented on the organization's IT systems.

(3) Protects the data the organization collects and uses.

(4) Safeguards the technology assets in use at the organization.

**Protecting the functionality of an organization**

- Decision makers in organizations must set policy and operate their organizations in compliance with the complex, shifting legislation that controls the use of technology.

**Enabling the safe operation of applications**

- Organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications
- The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly those applications that serve as important elements of the infrastructure of the organization.

**Protecting data that organizations collect & use**

- Protecting data in motion
- Protecting data at rest
- Both are critical aspects of information security.
- The value of data motivates attackers to seal, sabotage, or corrupts it.
- It is essential for the protection of integrity and value of the organization's data

**Safeguarding Technology assets in organizations**

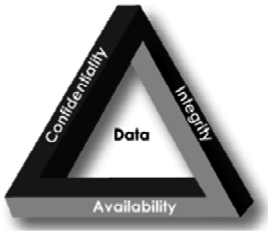
- Must add secure infrastructure services based on the size and scope of the enterprise.
- Organizational growth could lead to the need for **public key infrastructure,** PKI, an integrated system of software, encryption methodologies.

**Why your small business needs an information security policy**

Think you don't have anything of value to protect? Think again. The key asset that a security program helps to protect is your data — and the value of your business is in its data. You already know this if your company is one of many whose data management is dictated by governmental and other regulations — for example, how you manage customer credit card data. If your data management practices are not already covered by regulations, consider the value of the following:

- Product information, including designs, plans, patent applications, source code, and drawings
- Financial information, including market assessments and your company's own financial records
- Customer information, including confidential information you hold on behalf of customers or clients

Protecting your data means protecting its confidentiality, integrity, and availability as illustrated by the C-I-A triangle. The consequences of a failure to protect all three of these aspects include business losses, legal liability, and loss of company goodwill. Consider the following examples:




- Failure to protect your data's confidentiality might result in customer credit card numbers being stolen, with legal consequences and a loss of goodwill. Lose your clients' confidential information and you may have fewer of them in the future.
- A data integrity failure might result in a Trojan horse being planted in your software, allowing an intruder to pass your corporate secrets on to your competitors. If an integrity

failure affects your accounting records, you may no longer really know your company's true financial status.

Having a security program means that you've taken steps to mitigate the risk of losing data in any one of a variety of ways, and have defined a life cycle for managing the security of information and technology within your organization.

Hopefully the program is complete enough, and your implementation of the program is faithful enough, that you don't have to experience a business loss resulting from a security incident. If you have a security program and you do experience a loss that has legal consequences, your written program can be used as evidence that you were diligent in protecting your data and following industry best practices.

**Elements of a good security program**

A good security program provides the big picture for how you will keep your company's data secure. It takes a holistic approach that describes how every part of your company is involved in the program. A security program is not an incident handling guide that details what happens if a security breach is detected (see The Barking Seal Issue Q1 2006). It's also not a guide to doing periodic assessments, though it probably does dictate when to do a security assessment.

Your security program defines what data is covered and what is not. It assesses the risks your company faces, and how you plan to mitigate them. It indicates how often the program will be reevaluated and updated, and when you will assess compliance with the program. The key components of a good security program are outlined in the following sections.

**Designated security officer**

For most security regulations and standards, having a Designated Security Officer (DSO) is not optional - it's a requirement. Your security officer is the one responsible for coordinating and executing your security program. The officer is your internal check and balance. This person or role should report to someone outside of the IT organization to maintain independence.

**Risk assessment**

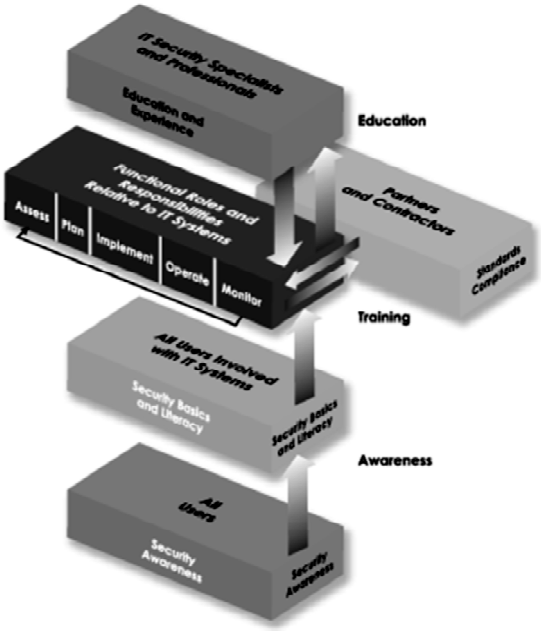
This component identifies and assesses the risks that your security program intends to manage. This is perhaps the most important section because it makes you think about the risks your organization faces so that you can then decide on appropriate, cost-effective ways to manage them. Remember that we can only minimize, not eliminate, risk, so this assessment helps us to prioritize them and choose cost-effective countermeasures. The risks that are covered in your assessment might include one or more of the following:

- Physical loss of data. You may lose immediate access to your data for reasons ranging from floods to loss of electric power. You may also lose access to your data for more subtle reasons: the second disk failure, for example, while your RAID array recovers from the first.
- Unauthorized access to your own data and client or customer data. Remember, if you have confidential information from clients or customers, you're often contractually obliged to protect that data as if it were your own.
- Interception of data in transit. Risks include data transmitted between company sites, or between the company and employees, partners, and contractors at home or other locations.
- Your data in someone else's hands. Do you share your data with third parties, including contractors, partners, or your sales channel? What protects your data while it is in their hands?
- Data corruption. Intentional corruption might modify data so that it favors an external party: think Trojan horses or keystroke loggers on PCs. Unintentional corruption might be due to a software error that overwrites valid data.

**Policies and Procedures**

Preparing your risk assessment hopefully gave you lots to worry about. The policies and procedures component is the place where you get to decide what to do about them. Areas that your program should cover include the following:

- Physical security documents how you will protect all three C-I-A aspects of your data from unauthorized physical access.
- Authentication, authorization, and accountability establish procedures for issuing and revoking accounts. It specifies how users authenticate, password creation and aging requirements, and audit trail maintenance.
- Security awareness makes sure that all users have a copy of your acceptable use policy and know their responsibilities; it also makes sure that your IT employees are engaged in implementing your IT-specific policies.
- Risk assessment states how often you will reassess the potential threats to your IT security and update your security program.
- Incident response defines how you will respond to security threats, including potential (such as unauthorized port scanning) and actual incidents (where security has been compromised). We discussed the importance of having an incident-handling guide in the Q1 2006 issue of The Barking Seal.
- Virus protection outlines how you protect against viruses. This might include maintaining workstation-based products and scanning email, Web content, and file transfers for malicious content.
- Business continuity planning includes how you will respond to various man-made and natural disaster scenarios. This includes setting up appropriate backup sites, systems, and data, as well as keeping them up-to-date and ready to take over within the recovery time you have defined.
- Relationships with vendors and partners defines who these organizations are, what kind of data you might exchange with them, and what provisions must be in your contracts to protect your data. This is an often-overlooked aspect of data security because your IT organization probably has not had a lot of interaction with your legal organization over vendor contracts. You may need to take measures such as evaluating your partners' ability to safeguard your data and insisting on having reasonable security practices in place.




## Organizational security awareness

The security community generally agrees that the weakest link in most organizations' security is the human factor, not technology. And even though it is the weakest link, it is often overlooked in security programs. Don't overlook it in yours.

Every employee needs to be aware of his or her roles and responsibilities when it comes to security. Even those who don't even touch a computer in their daily work need to be involved because they could still be targeted by social-engineering attacks designed to compromise your physical security. In its Information Security Handbook, publication 80-100, the National Institute of Standards and Technology (NIST) describes the importance of making all levels of your organization aware and educated on their roles and responsibilities when it comes to security. All users need to have security awareness training, while those involved with IT systems need to have more role-specific training. Your IT organization, which implements a continuous cycle of assessing, acquiring, and operating security-related hardware and software, needs even a higher level of involvement, taking direction from your own security specialists and those you hire as consultants.

**Regulatory standards compliance**

In addition to complying with your own security program, your company may also need to comply with one or more standards defined by external parties. This component of your security plan defines what those standards are and how you will comply. Regulatory standards that might affect you include HIPAA (for patient information), PCI (for credit card processing), FISMA (for governmental agencies and contractors, see The Barking Seal Q4 2006), Sarbanes-Oxley, and Gramm-Leach- Bliley (for corporate financial management).

**Audit compliance plan**

This component of your security program dictates how often you will audit your IT security and assess its compliance with your security program. As we discussed in the Q2 2008 issue of The Barking Seal, there are aspects of your security that you will want to audit on a frequency ranging from daily to annually. Periodic security assessments are important for finding out whether your security has already been breached. They help you to stay on top of new security threats with the right technology and staff training. And they help you make smart investments by helping you to prioritize and focus on the high-impact items on your list.

A security program is never done. As your IT organization is always in the process of iterating through the program's life cycle for all areas that it defines. You assess risks, make plans for mitigating them, implement solutions, monitor to be sure they are working as expected, and use that information as feedback for your next assessment phase. Likewise, your security program document has this life cycle built into it, as it specifies how often you will reassess the risks you face and update the program accordingly.

**Getting on the right footing**

It doesn't matter whether your security program is five pages (as are some we've produced for clients) or 200 pages long (such as the NIST document cited above). The important thing is that you have a security program and that you use it to address your company's security in an organized, comprehensive, and holistic way. You can adapt the above elements to create a security program for your organization, or, if you need help, give us a call at 303.245.4545.

Everyone needs to have a security program because it helps you maintain your focus on IT security. It helps you identify and stay in compliance with the regulations that affect how you manage your data. It keeps you on the right footing with your clients and your customers so that you meet both your legal and contractual obligations. Its life cycle process ensures that security is continuously adapting to your organization and the ever-changing IT environment we live in. And, of course, it's the right thing to do because protecting your data's security is the same as protecting your most important asset.

## 1.10 THREATS

**Q10. What are threats? Explain different categories of threats?**

*Ans :*

In Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

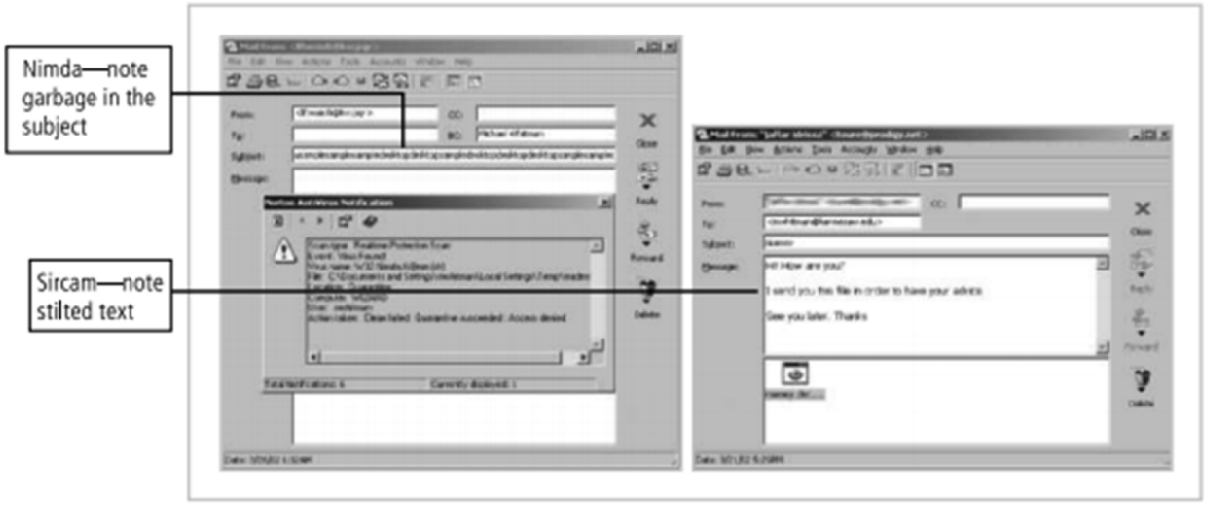
- **Threat** can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.
- **Software attacks** means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behave differently.

**Malware** is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or a anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

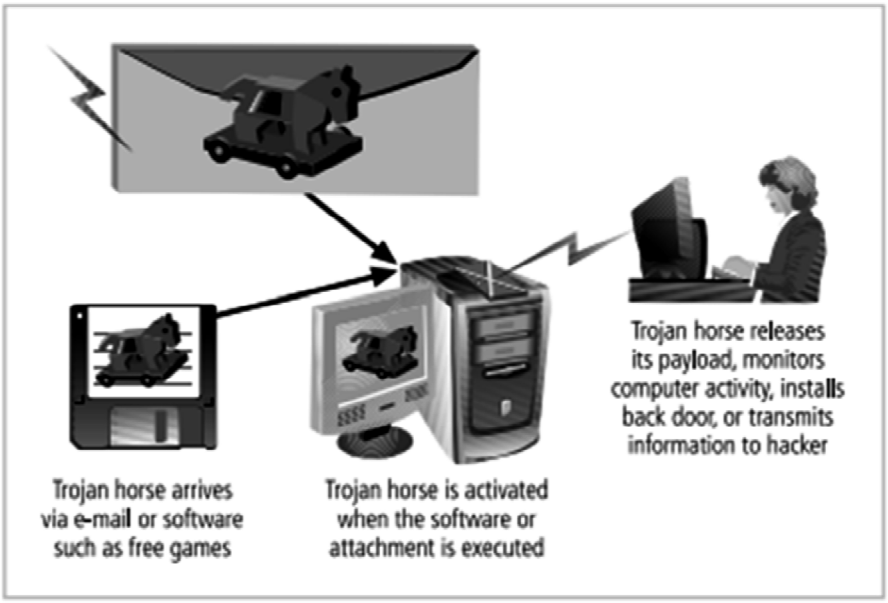
1. Infection Methods
2. Malware Actions

Malware on the **basis of Infection** Method are following:

- **Virus –** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. Ther Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
- **Worms –** Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will for example consume hard disk space thus slowing down the computer.




**3. Trojan –** The Concept of Trojan is completely different from the viruses and worms. The name Trojan derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.



Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.

They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, Remote Access Trojans etc.

4. **Bots –** can be seen as advanced for of worms. They are automated processes that are designed to interact over the internet without the need of human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**

**Malware on the basis of Actions:**

1. **Adware –** Adware is not exactly malicious but they do breach privacy of the users. They display ads on computer's desktop or inside individual programs. They come attached with free to use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
2. **Spyware –** It is a program or we can say a software that monitors your activities on computer and reveal collected information to interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they installs themselves and sits silently to avoid detection.
3. One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.
4. **Ransomware –** It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
5. **Scareware –** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
6. **Rootkits –** are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
7. **Zombies –** They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

- **Theft of intellectual property** means violation of intellectual property rights like copyrights, patents etc.
- **Identity theft** means to act someone else to obtain person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.
- **Theft of equipment and information** is increasing these days due to the mobile nature of devices and increasing information capacity.
- **Sabotage** means destroying company's website to cause loss of confidence on part of its customer.
- **Information extortion** means theft of company's property or information to receive payment in exchange. For example ransomware may lock victims file making them inaccessible thus forcing victim to make payment in exchange. Only after payment victim's files will be unlocked.

These are the old generation attacks that continue these days also with advancement every year. Apart from

these there are many other threats. Below is the brief description of these new generation threats.

- **Technology with weak security –** With the advancement in technology, with every passing day a new gadget is being released in the market. But very few are fully secured and follows Information Security principles. Since the market is very competitive Security factor is compromised to make device more up to date. This leads to theft of data/ information from the devices
- **Social media attacks –** In this cyber criminals identify and infect a cluster of websites that persons of a particular organisation visit, to steal information.
- **Mobile Malware –**There is a saying when there is a connectivity to Internet there will be danger to Security. Same goes to Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally they will install malware or virus in the device.
- **Outdated Security Software –** With new threats emerging everyday, updation in security software is a pre requisite to have a fully secured environment.
- **Corporate data on personal devices –** These days every organization follows a rule BYOD. BYOD means Bring your own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.
- **Social Engineering –** is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer. For example email or message from your friend, that was probably not sent by your friend. Criminal can access your friends device and then by accessing the contact list he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definately check the link or attachment in the message, thus unintentionally infecting the computer.

**Acts of Human Error or Failure:**

- Acts performed without intent or malicious purpose by an authorized user.
- because of in experience ,improper training,
- Making of incorrect assumptions.

One of the greatest threats to an organization's information security is the organization's own employees.

- Entry of erroneous data
- accidental deletion or modification of data
- storage of data in unprotected areas.
- Failure to protect information can be prevented with
  - Training
  - Ongoing awareness activities
  - Verification by a second party
  - Many military applications have robust, dual- approval controls built in .

**Compromises to Intellectual Property**

- Is defined as the ownership of ideas and control over the tangible or virtual representation of those ideas.
- Intellectual property includes trade secrets, copyrights, trademarks, and patents.
- Once intellectual property has been defined and properly identified, breaches to IP constitute a threat to the security of this information.

- Organization purchases or leases the IP of other organizations.
- Most Common IP breach is the unlawful use or duplication of software based intellectual property more commonly known as **software Piracy**.
- Software Piracy affects the world economy.
- U.S provides approximately 80% of world's software.

In addition to the laws surrounding software piracy, two watch dog organizations investigate allegations of software abuse.

1. Software and Information Industry Association (SIIA) (i.e)Software Publishers Association
2. Business Software Alliance (BSA)
   - Another effort to combat (take action against) piracy is the online registration process.

**Deliberate Acts of Espionage or Trespass**

- Electronic and human activities that can breach the confidentiality of information.
- When an unauthorized individual's gain access to the information an organization is trying to protect is categorized as act of espionage or trespass.
- Attackers can use many different methods to access the information stored in an information system.
  - i. Competitive Intelligence[use web browser to get information from market research]
  - ii. Industrial espionage(spying)
  - iii. Shoulder Surfing(ATM)

**Trespass**

- Can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.
- Sound principles of authentication & authorization can help organizations protect valuable information and systems.
- **Hackers-** People who use and create computer software to gain access to information illegally

There are generally two skill levels among hackers.

- **Expert Hackers**-Masters of several programming languages, networking protocols, and operating systems .
- **Unskilled Hackers**

**Deliberate Acts of information Extortion (obtain by force or threat)**

- Possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement not to disclose the information.

**Deliberate Acts of sabotage or Vandalism**

- Destroy an asset or
- Damage the image of organization
- Cyber terrorism-Cyber terrorists hack systems to conduct terrorist activities through network or internet pathways.

**Deliberate Acts of Theft**

- Illegal taking of another's property— is a constant problem.
- Within an organization, property can be physical, electronic, or intellectual.
- Physical theft can be controlled by installation of alarm systems.
- Trained security professionals.
- Electronic theft control is under research.

**Deliberate Software Attacks**

- Because of **malicious code** or **malicious software** or sometimes **malware.**
- These software components are designed to damage, destroy or deny service to the target system.
- More common instances are

- Virus, Worms, Trojan horses, Logic bombs, Backdoors.
- The British Internet Service Provider Cloudnine be the first business hacked out of existence

## 1.11 ATTACKS

**Q11. What deliberate software attack? Explain in detail different types of cryptanalytic attacks?**

*Ans :*

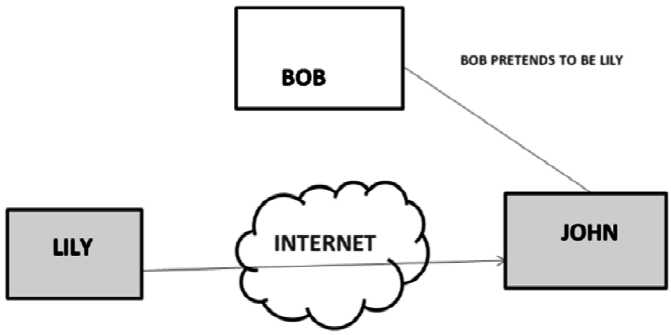
An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations. There are many different kinds of attacks, including but not limited to passive, active, targeted, clickjacking, brandjacking, botnet, phishing, spamming, inside and outside.

An attack is one of the biggest security threats in information technology, and it comes in different forms. A passive attack is one that does not affect any system, although information is obtained. A good example of this is wiretapping. An active attack has the potential to cause major damage to an individual's or organization's resource because it attempts to alter system resources or affect how they work. A good example of this might be a virus or other type of malware.

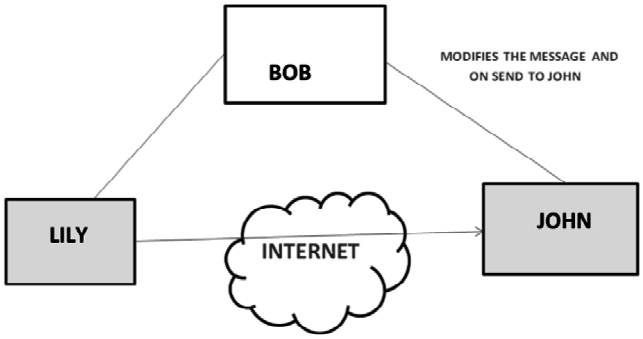
**Types of Security attacks**

**Active attacks:** An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:

**Masquerade –** Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.

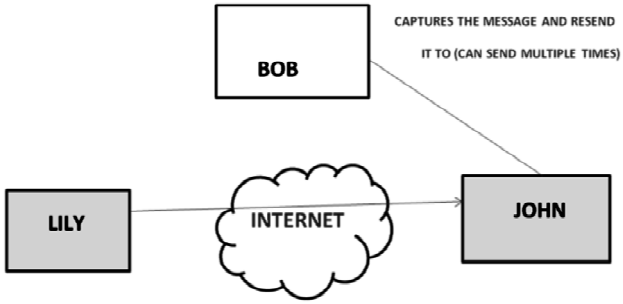



**Modification of messages –** It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning Allow JOHN to read confidential file X is modified as Allow Smith to read confidential file X .

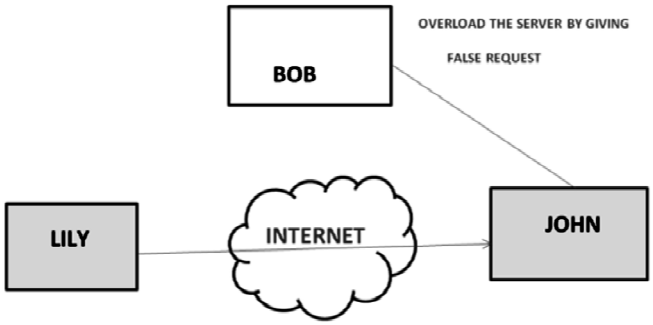


**Repudiation –** This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank To transfer an amount to someone and later on the sender(customer) deny that he had made such a request. This is repudiation.

i. **Replay –**It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.

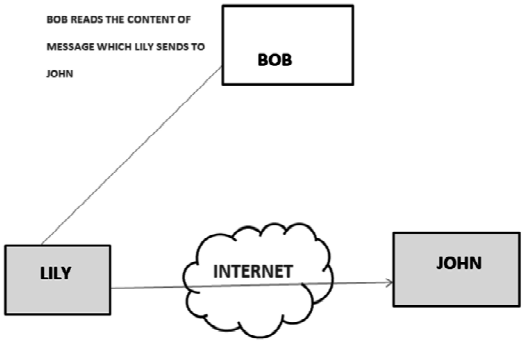



ii. **Denial of Service –** It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



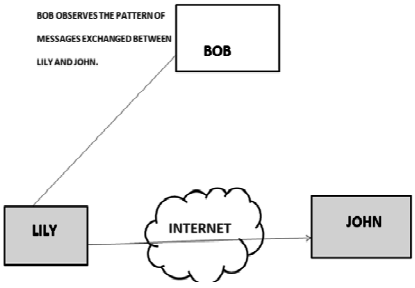

**Passive attacks:** A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

i. **The release of message content –** Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



ii. **Traffic analysis –** Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.

The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.




**Antivirus Program**

A Utility that searches a hard disk for viruses and removes any that found.

**Forces of Nature**

- **Fire:** Structural fire that damages the building. Also encompasses smoke damage from a fire or water damage from sprinkles systems.
- **Flood:** Can sometimes be mitigated with flood insurance and/or business interruption Insurance.
- **Earthquake:** Can sometimes be mitigated with specific causality insurance and/or business interruption insurance, but is usually a separate policy.
- **Lightning**: An Abrupt, discontinuous natural electric discharge in the atmosphere.
- **Landslide/Mudslide**: The downward sliding of a mass of earth & rocks directly damaging all parts of the information systems.
- **Tornado/Severe Windstorm:**
- **Huricane/typhoon**
- **Tsunami**
- **Electrostatic Discharge (ESD)**
- **Dust Contamination**

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage.

They must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans, to limit losses in the face of these threats.

**Deviations in Quality of Service**

- A product or service is not delivered to the organization as expected.
- The Organization's information system depends on the successful operation of many interdependent support systems.

- It includes power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff & garbage haulers.
- This degradation of service is a form of **availability disruption.**

**Internet Service Issues**

- Internet service Provider(ISP) failures can considerably undermine the availability of information.
- The web hosting services are usually arranged with an agreement providing minimum service levels known as a **Service level Agreement (SLA).**
- When a Service Provider fails to meet SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

**Communications & Other Service Provider Issues**

- Other utility services can affect the organizations are telephone, water, waste water, trash pickup, cable television, natural or propane gas, and custodial services.
- The loss of these services can impair the ability of an organization to function.
- For an example, if the waste water system fails, an organization might be prevented from allowing employees into the building.
- This would stop normal business operations.

**Power Irregularities**

- Fluctuations due to power excesses.
- Power shortages & Power losses

  This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.
- When voltage levels **spike** (experience a momentary increase),or **surge** ( experience prolonged increase ), the extra voltage can severely damage or destroy equipment.
- The more expensive uninterruptible power supply (UPS) can protect against spikes and surges.

**Technical Hardware Failures or Errors**

- Resulting in unreliable service or lack of availability
- Some errors are terminal, in that they result in unrecoverable loss of equipment.
- Some errors are intermittent, in that they resulting in faults that are not easily repeated.

**Technical software failures or errors**

- This category involves threats that come from purchasing software with unknown, hidden faults.
- Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.
- These failures range from bugs to untested failure conditions.

**Technological obsolescence**

- Outdated infrastructure can lead to unreliable and untrustworthy systems.
- Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks.

**Man-in-the –Middle**

- Otherwise called as **TCP hijacking attack**.
- An attacker monitors packets from the network, modifies them, and inserts them back into the network.
- This type of attack uses IP spoofing.
- It allows the attacker to change, delete, reroute, add, forge or divert data.
- TCP hijacking session, the spoofing involves the interception of an encryption key exchange.

**SPAM**

- Spam is unsolicited commercial E-mail.

- It has been used to make malicious code attacks more effective.
- Spam is considered as a trivial nuisance rather than an attack.
- It is the waste of both computer and human resources it causes by the flow of unwanted E-mail.

**Mail Bombing**

- Another form of E-mail attack that is also a DOS called a **mail bomb**.
- Attacker routes large quantities of e-mail to the target.
- The target of the attack receives unmanageably large volumes of unsolicited e-mail.
- By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.
- The target e-mail address is buried under thousands or even millions of unwanted emails.

**Sniffers**

- A **sniffer** is a program or device that can monitor data traveling over a network.
- Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere.
- Sniffer often works on TCP/IP networks, where they are sometimes called **packet** Sniffers .

**Social Engineering**

- It is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.
- An attacker gets more information by calling others in the company and asserting his/her authority by mentioning chief's name.

**Buffer Overflow**

- A buffer overflow is an application error that occurs when more data is sent to a buffer than it can handle.
- Attacker can make the target system execute instructions.

**Timing Attack**

- Works by exploring the contents of a web browser's cache.
- These attacks allow a Web designer to create a malicious form of cookie that is stored on the client's system.

  The cookie could allow the designer to collect information on how to access password-protected sites.

### 1.11.1 Other Attacks

- An attack is an act of or action that takes advantage of a vulnerability to compromise a controlled system.
- It is accomplished by a **threat agent** that damages or steals an organization's information or physical asset.
- **Vulnerability** is an identified weakness in a controlled system, where controls are not present or are no longer effective.
- Attacks exist when a specific act or action comes into play and may cause a potential loss.

**Malicious code**

- The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
- The state –of-the-art malicious code attack is the polymorphic or multivector, worm.
- These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

**Attack Replication Vectors**

1. **IP scan & attack -** The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers.
2. **Web browsing -** If the infected system has write access to any Web pages, it makes all Web content files (.html,.asp,.cgi & others) infectious, so that users who browse to those pages become infected.
3. **Virus -** Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.
4. **Unprotected shares-** Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.
5. **Mass Mail -** By sending E-mail infections to addresses found in the address book, the infected machine infects many users, whose mail -reading programs also automatically run the program & infect other systems.
6. **Simple Network Management Protocol (SNMP) -** By using the widely known and common passwords that were employed in early versions of this protocol, the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.
7. **Hoaxes**
   - A more devious approach to attacking the computer systems is the transmission of a virus hoax with a real virus attached.
   - Even though these users are trying to avoid infection, they end up sending the attack on to their co-workers.
8. **Backdoors**
   - Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door.
   - Sometimes these entries are left behind by system designers or maintenance staff, and thus referred to as trap doors.
   - A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.
9. **Password Crack**
   - Attempting to reverse calculate a password is often called **cracking.**
   - A password can be hashed using the same algorithm and compared to the hashed results, If they are same, the password has been cracked.
   - The (SAM) Security Account Manager file contains the hashed representation of the user's password.
10. **Brute Force**
    - The application of computing & network resources to try every possible combination of options of a password is called a **Brute force attack.**
    - This is often an attempt to repeatedly guess passwords to commonly used accounts, it is sometimes called a **password attack.**
11. **Dictionary**
    - This is another form of the brute force attack noted above for guessing passwords.
    - The **dictionary attack** narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords instead of random combinations.
12. **Denial -of- Services(DOS) & Distributed Denial –of- Service(DDOS)**
    - The attacker sends a large number of connection or information requests to a target.
    - This may result in the system crashing, or simply becoming unable to perform ordinary functions.

- DDOS is an attack in which a coordinated stream of requests is launched against a target from many locations at the same.

**13. Spoofing-** It is a technique used to gain unauthorized access to computers, where in the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host.

## 1.12 Secure Development Lifecycle

**Q12. Explain the principles & Development of Sec Development life cycle of software.**

*Ans :*

### Secure Software Development

Secure Software Development Systems consist of hardware, software, networks, data, procedures, and people using the system. Many of the information security issues described in this chapter have their root cause in the software elements of the system. Secure systems require secure, or at least securable, software. The development of systems and the software they use is often accomplished using a methodology, such as the systems development life cycle (SDLC). Many organizations recognize the need to include planning for security objectives in the SDLC they use to create systems, and have put in place procedures to create software that is more able to be deployed in a secure fashion. This approach to software development is known as software assurance, or SA.

### Software Assurance and the SA Common Body of Knowledge

Organizations are increasingly working to build security into the systems development life cycle, to prevent security problems before they begin. A national effort is underway to create a common body of knowledge focused on secure software development. The U.S. Department of Defense (DoD) launched a Software Assurance Initiative in 2003. This initial process was led by Joe Jarzombek and was endorsed and supported by the Department of Homeland Security (DHS), which joined the program in 2004. This program initiative resulted in the publication of the Secure Software Assurance (SwA) Common Body of Knowledge (CBK). A working group drawn from industry, government, and academia was formed to examine two key questions:

1. What are the engineering activities or aspects of activities that are relevant to achieving secure software?
2. What knowledge is needed to perform these activities or aspects?

Based on the findings of this working group, and a host of existing external documents and standards, the SwA CBK was developed and published to serve as a guideline. While this work has not yet been adopted as a standard or even a policy requirement of government agencies, it serves as a strongly recommended guide to developing more secure applications. The SwA CBK, which is a work in progress, contains the following sections:

- Nature of Dangers
- Fundamental Concepts and Principles
- Ethics, Law, and Governance
- Secure Software Requirements
- Secure Software Design
- Secure Software Construction
- Secure Software Verification, Validation, and Evaluation
- Secure Software Tools and Methods
- Secure Software Processes
- Secure Software Project Management
- Acquisition of Secure Software
- Secure Software Sustainment.

The following sections provides insight into the stages that should be incorporated into the software SDLC.

### Software Design Principles

Good software development should result in a finished product that meets all of its design specifications. Information security considerations are a critical component of those specifications, though that has not always been true. Leaders in software development J. H. Saltzer and M. D. Schroeder note that. This statement could be about software development in the early part of the 21st

century, but actually dates back to 1975, before information security and software assurance became critical factors for many organizations. In this same article, the authors provide insight into what are now commonplace security principles:

- **Economy of mechanism:** Keep the design as simple and small as possible.
- **Fail-safe defaults:** Base access decisions on permission rather than exclusion.
- **Complete mediation:** Every access to every object must be checked for authority.
- **Open design:** The design should not be secret, but rather depend on the possession of keys or passwords.
- **Separation of privilege:** Where feasible, a protection mechanism should require two keys to unlock, rather than one.
- **Least privilege:** Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- **Least common mechanism:** Minimize mechanisms (or shared variables) common to more than one user and depended on by all users.
- **Psychological acceptability:** It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.
- **Software Development Security Problems:** Some software development problems that result in software that is difficult or impossible to deploy in a secure fashion have been identified as deadly sins in software security. These twenty problem areas in software development (which is also called software engineering) were originally categorized by John Viega, upon request of Amit Youran, who at the time was the Director of the Department of Homeland Security's National Cyber Security Division.
- **Buffer Overruns:** Buffers are used to manage mismatches in the processing rates between two entities involved in a communication process. A buffer overrun (or buffer overflow) is an application error that occurs when more data is sent to a program buffer than it is designed to handle. During a buffer overrun, an attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure. Sometimes this is limited to a denial-of-service attack. In any case, data on the attacked system loses integrity.

  Command Injection Command injection problems occur when user input is passed directly to a compiler or interpreter. The underlying issue is the developer's failure to ensure that command input is validated before it is used in the program. Perhaps the simplest example involves the Windows command shell:

```
@echo off
set /p myVar= Enter the string>
set someVar=%myVar%
echo %somevar%
```

  These simple commands ask the user to provide a string and then simply set another variable to the value and then display it. However, an attacker could use the command chaining character & to append other commands to the string the user provides (Hello&del*.*).

- **Failure to Handle Errors:** What happens when a system or application encounters an scenario that it is not prepared to handle? Does it attempt to complete the operation (reading or writing data or performing calculations)? Does it issue a cryptic message that only a programmer could understand? Or does it simply stop functioning? Failure to handle errors can cause a variety of unexpected system behaviors. Programmers are expected to anticipate problems and prepare their application code to handle them.
- **Failure to Protect Network Traffic:** With the growing popularity of wireless networking

comes a corresponding increase in the risk that wirelessly transmitted data will be intercepted. Most wireless networks are installed and operated with little or no protection for the information that is broadcast between the client and the network wireless access point. This is especially true of public networks found in coffee shops, bookstores, and hotels. Without appropriate encryption (such as that afforded by WPA), attackers can intercept and view your data. Traffic on a wired network is also vulnerable to interception in some situations. On networks using hubs instead of switches, any user can install a packet sniffer and collect communications to and from users on that network. Periodic scans for unauthorized packet sniffers, unauthorized connections to the network, and general awareness of the threat can mitigate this problem.

- **Failure to Store and Protect Data Securely:** Storing and protecting data securely is a large enough issue to be the core subject of this entire text. Programmers are responsible for integrating access controls into, and keeping secret information out of, programs. Access controls, the subject of later chapters, regulate who, what, when, where, and how individuals and systems interact with data. Failure to properly implement sufficiently strong access controls makes the data vulnerable. Overly strict access controls hinder business users in the performance of their duties, and as a result the controls may be administratively removed or bypassed. The integration of secret information—such as the hard coding of passwords, encryption keys, or other sensitive information—can put that information at risk of disclosure.

- **Failure to Use Cryptographically Strong Random Numbers:** Most modern cryptosystems, like many other computer systems, use random number generators. However, a decision support system using random and pseudo-random numbers for Monte Carlo method forecasting does not require the same degree of rigor and the same need for true randomness as a system that seeks to implement cryptographic procedures. These random number generators use a mathematical algorithm, based on a seed value and another other system component (such as the computer clock) to simulate a random number. Those who understand the workings of such a random number generator can predict particular values at particular times.

- **Format String Problems:** Computer languages often are equipped with built-in capabilities to reformat data while they're outputting it. The formatting instructions are usually written as a format string. Unfortunately, some programmers may use data from untrusted sources as a format string. An attacker may embed characters that are meaningful as formatting directives (e.g., %x, %d, %p, etc.) into malicious input; if this input is then interpreted by the program as formatting directives (such as an argument to the C printf function), the attacker may be able to access information or overwrite very targeted portions of the program's stack with data of the attacker's choosing.

- **Neglecting Change Control:** Developers use a process known as change control to ensure that the working system delivered to users represents the intent of the developers. Early in the development process, change control ensures that developers do not work at cross purposes by altering the same programs or parts of programs at the same time. Once the system is in production, change control processes ensure that only authorized changes are introduced and that all changes are adequately tested before being released.

- **Improper File Access:** If an attacker changes the expected location of a file by intercepting and modifying a program code call, the attacker can force a program to use files other than the ones the program is supposed to use. This type of attack could be used to either substitute a bogus file for a legitimate file (as in password files), or trick the system into running a malware executable.

The potential for damage or disclosure is great, so it is critical to protect not only the location of the files but also the method and communications channels by which these files are accessed.

- **Information Leakage:** One of the most common methods of obtaining inside and classified information is directly or indirectly from an individual, usually an employee. The World War II military poster warned that loose lips sink ships, emphasizing the risk to naval deployments from enemy attack should the sailors, marines, or their families disclose the movements of these vessels. It was a widely-shared fear that the enemy had civilian operatives waiting in bars and shops at common Navy ports of call, just waiting for the troops to drop hints about where they were going and when. By warning employees against disclosing information, organizations can protect the secrecy of their operation.

- **Unauthenticated Key Exchange:** One of the biggest challenges in private key systems, which involve two users sharing the same key, is securely getting the key to the other party. Sometimes an out of band courier is used, but other times a public key system, which uses both a public and private key, is used to exchange the key. But what if the person who receives a key that was copied onto a USB device and shipped doesn't really work for the company, but was simply expecting that particular delivery and intercepted it? The same scenario can occur on the Internet, where an attacker writes a variant of a public key system and places it out as freeware, or corrupts or intercepts the function of someone else's public key encryption system, perhaps by posing as a public key repository.

**Use of Weak Password:** Based Systems Failure to require sufficient password strength, and to control incorrect password entry, is a serious security issue. Password policy

| Password Length | Maximum Number of Operations (guesses) | Maximum Time to Crack |
|---|---|---|
| 8 | 208,827,064,576 | 7.0 seconds |
| 9 | 5,429,503,678,976 | 3.0 minutes |
| 10 | 141,167,095,653,376 | 1.3 hours |
| 11 | 3,670,344,486,987,780 | 34.0 hours |
| 12 | 95,428,956,661,682,200 | 36.8 days |
| 13 | 2,481,152,873,203,740,000 | 2.6 years |
| 14 | 64,509,974,703,297,200,000 | 68.2 years |
| 15 | 1,677,259,342,285,730,000,000 | 1,772.9 years |
| 16 | 43,608,742,899,428,900,000,000 | 46,094.1 years |

**Using an extended data set with case sensitive letters (upper and lower case), numbers, and 20 special characters = 82 characters in set, on the same 2008-era dual-core PC:**

| Password Length | Maximum Number of Operations (guesses) | Maximum Time to Crack |
|---|---|---|
| 8 | 2,044,140,858,654,980 | 18.9 hours |
| 9 | 167,619,550,409,708,000 | 64.7 days |
| 10 | 13,744,803,133,596,100,000 | 14.5 years |
| 11 | 1,127,073,856,954,880,000,000 | 1,191.3 years |
| 12 | 92,420,056,270,299,900,000,000 | 97,687.4 years |
| 13 | 7,578,444,614,164,590,000,000,000 | 8,010,363.4 years |
| 14 | 621,432,458,361,496,000,000,000,000 | 656,849,799.6 years |
| 15 | 50,957,461,585,642,700,000,000,000,000 | 53,861,683,563.4 years |
| 16 | 4,178,511,850,022,700,000,000,000,000,000 | 4,416,658,052,197.2 years |

can specify the number and type of characters, the frequency of mandatory changes, and even the reusability of old passwords. Similarly, a system administrator can regulate the permitted number of incorrect password entries that are submitted and further improve the level of protection. Systems that do not validate passwords, or store passwords in easy-to-access locations, are ripe for attack. As shown in Table, the strength of a password determines its ability to withstand a brute force attack. Using non-standard password components can greatly enhance the strength of the password.

**Poor Usability**

Employees prefer doing things the easy way. When faced with an official way of performing a task and an unofficial way — which is easier—they prefer the easier method. The only way to address this issue is to only provide one way—the secure way! Integrating security and usability, adding training and awareness, and ensuring solid controls all contribute to the security of information. Allowing users to default to easier, more usable solutions will inevitably lead to loss.

### 1.12.1 Security Solutions for Software Development

The following is an extensive library of security solutions guides that are meant to be helpful and informative resources on a range of security solutions topics, from web application security to information and network security solutions to mobile and internet security solutions.

- **Code Security-** Analysis Security is a major aspect of business competitiveness today. A major attack on the enterprise can reduce productivity, tie up resources, harm credibility and cut into profits.
- **Cyber Security-** Many companies and countries understand that cyber threat is one of the most serious economic security challenges they face and that their economic prosperity depends on cyber security.
- **Ethical Hacking-** Computer hacking is a practice with many nuances. Intent, whether benign or malicious, is often in the eyes of the beholder. When examining the root cause of a website hack or application exploit, it pays to follow the money.
- **Facebook Security**- User's guide to Facebook Application Security. Get tips to protect your Facebook account from security flaws.
- **Firewall Security**- The term firewall originated to describe a building wall that offers physical protection from damaging fire. Firewall security technology, first introduced to computer networks in the late 1980s, protects private networks by securing gateway servers to external networks like the internet.
- **Flash Security-** Flash has a long record of critical security updates aimed at patching flash vulnerabilities and flash malware, but these issues continue to surface as more flash security issues are discovered.
- **Information Technology Infrastructure Library (ITIL) -** The Information Technology Infrastructure Library (ITIL) is an amassed collection of information that contains guidelines about how to create best practice infrastructure in the IT management of your organization.
- **Internet Security -** The internet represents an insecure channel for exchanging information, leading to a high risk of intrusion or fraud.
- **JavaScript Security** - JavaScript is a high-level, interpreted programming language that has been widely used since its release in 1995. Since its release, there have been several JavaScript security issues that have gained widespread attention.

- **Linux Hacking -** Linux is an open source operating system for computers. Linux is a Unix-like operating system, meaning that it supports multitasking and multi-user operation. Linux is widely used for supercomputers, mainframe computers and servers.
- **Packet Analyzer** - Packet analyzers are used to monitor, intercept and decode data packets as they are transmitted across networks.
- **Password Hacking** - Any way you look at it: your secret passwords are under attack. Computer hackers love to successfully defeat cryptography systems. Cybercriminals enjoy getting access to your online accounts.
- **Ruby Security** - Just like security applications with other frameworks, securing Ruby apps requires a mix of utilizing best practices in coding along with correctly using helper methods that are provided to help protect against certain types of attacks.
- **Secure Development**- With the vast amount of threats that constantly pressure companies and governments, it is important to ensure that the software applications these organizations utilize are completely secure.
- **Software Audit** - There are many ways to audit a software application. Indeed, the most basic kinds of software audits examine how the software is functionally configured, integrated or utilized within an organization.
- **Software Code Security** - The key to achieving superior software code security is to find a solution that can review large amounts of code as needed, in order to meet development timelines.
- **Software Development Lifecycle (SDLC) -** SDLC stands for software development lifecycle. A software development lifecycle is essentially a series of steps, or phases, that provide a model for the development and lifecycle management of an application or piece of software.
- **Software Security** - By testing for flaws in software, security testing solutions seek to remove vulnerabilities before software is purchased or deployed — and before the flaws can be exploited.
- **Software Testing Process** - As the enterprise network has become more secure, attackers have turned their attention to the application layer, which, according to Gartner, now contains 90 percent of all vulnerabilities.
- **Wireless Sniffer** - A wireless sniffer is a type of packet analyzer. A packet analyzer (also known as a packet sniffer) is a piece of software or hardware designed to intercept data as it is transmitted over a network and decode the data into a format that is readable for humans.

UNIT II

**Legal, Ethical and professional Issues:** Law and ethics in information security, Relevant U.S lawsinternational laws and legal bodies, Ethics and information security.

**Risk Management:** Overview, Risk identification, Risk assessment, Risk control strategies, selecting a risk control strategy, Quantitive versus qualitative risk control practices, Risk management discussion points, Recommended risk control practices.

## 2.1 Laws and Ethics

**Q1. Explain different types of laws & ethics in information security**

*Ans :*

Information is power. Nowadays, main concern of cyber community is to protect this valuable asset. Technical and technological security measures are sometimes insufficient to protect an information system. Because there is a human factor in information system. Ethics are set of moral rules that guide people. With the help of ethics a better and robust security can be achieved. In this paper role of ethics in information security is discussed. First of all law, ethics and information security concepts are briefly introduced. Later, some ethical concerns and perspectives in information security are given. To emphasize role of ethics in information security, several studies are reviewed. Finally, mechanisms to make ethical rules effective in an organization/community are discussed with several case studies.

**Law and Ethics in Information Security**

As a future information security professional, it is vital that you understand the scope of an organization's legal and ethical responsibilities. To minimize the organization's liabilities the information security practitioner must understand the current legal environment and keep apprised of new laws, regulations, and ethical issues as they emerge.

By educating employees and management about their legal and ethical obligations and the proper use of information technology and information security, security professionals can keep an organization focused on its primary objectives.

- Laws are rules adopted and enforced by governments to codify expected behavior in modern society.
- The key difference between law and ethics is that law carries the sanction of a governing authority and ethics do not.
- Ethics are based on cultural mores: relatively fixed moral attitudes or customs of a societal group.

**The Legal Environment**

- The information security professional and managers involved in information security must possess a rudimentary grasp of the legal framework within which their organizations operate.
- This legal environment can influence the organization to a greater or lesser extent depending on the nature of the organization and the scale on which it operates.

**Types of Law**

- Civil law embodies a wide variety of laws pertaining to relationships between and among individuals and organizations.
- Criminal law addresses violations harmful to society and is actively enforced and prosecuted by the state.
- Tort law is a subset of civil law which allows individuals to seek recourse against others in the event of personal, physical, or financial injury.
- Private law regulates the relationships among individuals and among individuals and organizations, and encompasses family law, commercial law, and labor law.

- Public law regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments.
- Public law includes criminal, administrative, and constitutional law.

## 2.2 Relevant U.S. Laws

**Q2. Explain differnt U.S. laws based on computer crimes?**

*Ans :*

| ACT | SUBJECT | DATE | DESCRIPTION |
|---|---|---|---|
| Communications Act of 1934, updated by Tele communi-cations Deregulation & Com-petition Act | Telecommunications | 1934 | Regulates interstate and foreign Tele-communications. |
| Computer Fraud & Abuse Act | Threats to computers | 1986 | Defines and formalizes laws to counter threats from computer related acts and offenses. |
| Computer Security Act of 1987 | Federal Agency Information Security | 1987 | Requires all federal computer systems that contain classified information to have surety plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems. |
| Economic Espionage Act of 1996 | Trade secrets. | 1996 | Designed to prevent abuse of information gained by an individual working in one company and employed by another. |
| Electronic Communi cations Privacy Act of 1986 | Cryptography | 1986 | Also referred to as the Federal Wiretapping Act; regulates interception and disclosure of electronic infor- mation. |
| Federal Privacy Act of 1974 | Privacy | 1974 | Governs federal agency use of personal information. |
| Gramm – Leach - Bliley Act of 1999 | Banking | 1999 | Focuses on facilitating affiliation among banks, insurance and securities firms; it has significant impact on the privacy of personal information used by these industries. |
| Health Insurance Portability and Accountability Act | Health care privacy | 1996 | Regulates collection, storage, and transmission of sensitive personal health care information. |
| National Information Infrastru cture protection Act of 1996 | Criminal intent | 1996 | Categorized crimes based on defendant's authority to access computer and criminal intent. |
| Sarbanes-Oxley Act of 2002 | Financial Reporting | 2002 | Affects how public organizations and accounting firms deal with corporate governance, financial disclosure, and the practice of public accounting. |
| Security and Freedom through Encryption Act of 19 99 | Use and sale of software that uses or enables encryption. | 1999 | Clarifies use of encryption for people in the United states and permits all persons in the U.S. to buy or sell any encryption product and states that the government cannot require the use of any kind of key escrow system for encryption products. |
| U.S.A. Patriot Act of 2001 | Terrorism | 2001 | Defines stiffer penalties for prosecution of terrorist crimes. |

## 2.3 International Laws and Legal Bodies

**Q3. What are international laws on laws & legal bodies?**

*Ans :*

The Computer Fraud and Abuse Act of 1986 (CFA Act) is the cornerstone of many computer-related federal laws and enforcement efforts.

It was amended in October 1996 by the National Information Infrastructure Protection Act of 1996, which modified several sections of the previous act, and increased the penalties for selected crimes.

The CFA Act was further modified by the USA Patriot Act of 2001-the abbreviated name for "Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," which provides law enforcement agencies with broader latitude to combat terrorism-related activities. Some of the laws modified by the Patriot Act date from the earliest laws created to deal with electronic technology.

The Communication Act of 1934 was revised by the Telecommunications Deregulation and Competition Act of 1996, which attempts to modernize the archaic terminology of the older act.

The Computer Security Act of 1987 was one of the first attempts to protect federal computer systems by establishing minimum acceptable security practices.

The Computer Security Act of 1987 charged the National Bureau of Standards, in cooperation with the National Security Agency, with the following tasks:

- Developing standards, guidelines, and associated methods and techniques for computer systems
- Developing uniform standards and guidelines for most federal computer systems
- Developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in federal computer systems
- Developing guidelines for use by operators of federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice
- Developing validation procedures for, and evaluate the effectiveness of, standards and guidelines through research and liaison with other government and private agencies.

The Computer Security Act also established a Computer System Security and Privacy Advisory Board within the Department of Commerce.

The Computer Security Act of 1987 also amended the Federal Property and Administrative Services Act of 1949, requiring the National Bureau of Standards to distribute standards and guidelines pertaining to federal computer systems, making such standards compulsory and binding to the extent to which the secretary determines necessary to improve the efficiency of operation or security and privacy of federal computer systems.

Another provision of the Computer Security Act requires mandatory periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of each federal computer system.

**Privacy Laws**

Many organizations collect, trade, and sell personal information as a commodity, and many individuals are becoming aware of these practices and looking to the governments to protect their privacy.

In the past it was not possible to create databases that contained personal information collected from multiple sources.

Today, the aggregation of data from multiple sources permits unethical organizations to build databases with alarming quantities of personal information.

The Privacy of Customer Information Section of the section of regulations covering common carriers specifies that any proprietary information shall be used explicitly for providing services, and not for any marketing purposes.

The Federal Privacy Act of 1974 regulates the government's use of private information. The Federal Privacy Act was created to ensure that government agencies protect the privacy of individuals' and businesses' information, and holds those agencies responsible if any portion of this information is released without permission.

The Electronic Communications Privacy Act of 1986 is a collection of statutes that regulates the interception of wire, electronic, and oral communications.

These statutes work in cooperation with the Fourth Amendment of the U.S. Constitution, which prohibits search and seizure without a warrant.

The Health Insurance Portability & Accountability Act Of 1996 (HIPPA), also known as the Kennedy-Kassebaum Act, is an attempt to protect the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange.

HIPPA requires organizations that retain health care information to use information security mechanisms to protect this information, as well as policies and procedures to maintain them, and also requires a comprehensive assessment of the organization's information security systems, policies, and procedures. HIPPA provides guidelines for the use of electronic signatures based on security standards ensuring message integrity, user authentication, and non-repudiation.

**HIPPA has five fundamental privacy principles:**

1. Consumer control of medical information
2. Boundaries on the use of medical information
3. Accountability for the privacy of private information
4. Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
5. Security of health information

The Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999 contains a number of provisions that affect banks, securities firms, and insurance companies.

This act requires all financial institutions to disclose their privacy policies, describing how they share nonpublic personal information, and describing how customers can request that their information not be shared with third parties.

The act also ensures that the privacy policies in effect in an organization are fully disclosed when a customer initiates a business relationship, and distributed at least annually for the duration of the professional association.

**Export and Espionage Laws**

- In an attempt to protect intellectual property and competitive advantage, Congress passed the Economic Espionage Act (EEA) in 1996.
- This law attempts to protect trade secrets "from the foreign government that uses its classic espionage apparatus to spy on a company, to the two American companies that are attempting to uncover each other's bid proposals, or to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics."


The Security and Freedom through Encryption Act of 1997 provides guidance on the use of encryption, and institutes measures of public protection from government intervention. Specifically, the Act reinforces an individual's right to use or sell encryption algorithms, without concern for the impact of other regulations requiring some form of key registration and prohibits the federal government from requiring the use of encryption for contracts, grants, and other official documents, and correspondence.

**U.S. Copyright Law**

U.S. copyright law extends protection to intellectual property, which includes words published in electronic formats.

The doctrine of fair use allows material to be quoted for the purpose of news reporting, teaching, scholarship, and a number of other related activities, so long as the purpose is educational and not for profit, and the usage is not excessive.

Proper acknowledgement must be provided to the author and/or copyright holder of such works, including a description of the location of source materials by using a recognized form of citation.

**Freedom of Information Act of 1966 (FOIA)**

All federal agencies are required under the Freedom of Information Act (FOIA) to disclose records requested in writing by any person.

The FOIA applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies.

**Sarbanes-Oxley Act of 2002**

The U.S. Congress enacted the Sarbanes-Oxley Act of 2002 to enforce accountability for the financial record keeping and reporting at publicly traded corporations.

The law requires that the CEO and chief financial officer (CFO) assume direct and personal accountability for the completeness and accuracy of a publicly traded organization's financial reporting and record-keeping systems.

As these executives attempt to ensure that the systems used to record and report are sound-often relying upon the expertise of CIOs and CISOs to do so-the related areas of availability and confidentiality are also emphasized.

**International Laws and Legal Bodies**

Many domestic laws and customs do not apply to international trade, which is governed by international treaties and trade agreements.

Because of the political complexities of the relationships among nations and cultural differences, there are currently few international laws relating to privacy and information security.

**European Council Cyber-Crime Convention**

Recently the Council of Europe drafted the European Council Cyber-Crime Convention, which empowers an international task force to oversee a range of Internet security functions, and to standardize technology laws across international borders.

It also attempts to improve the effectiveness of international investigations into breaches of technology law.

The overall goal of the convention is to simplify the acquisition of information for law enforcement agents in certain types of international crimes, as well as the extradition process.

**Digital Millennium Copyright Act (DMCA)**

The Digital Millennium Copyright Act (DMCA) is a U.S.-based international effort to reduce the impact of copyright, trademark, and privacy infringement especially via the removal of technological copyright protection measures.

The European Union also put forward Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 that increases individual rights to process and freely move personal data.

The United Kingdom has already implemented a version of this directive called the Database Right.

**State and Local Regulations**

It is the responsibility of information security professionals to understand state laws and regulations and ensure that their organization's security policies and procedures comply with the laws and regulations.

For example, the State of Georgia recently passed the Georgia Computer Systems Protection Act, which has various computer security provisions, and establishes specific penalties for use of information technology to attack or exploit information systems in organizations.

The Georgia legislature also passed the Georgia Identity Theft Law in 1998, which requires that a business may not discard a record containing personal information unless it, shreds, erases, modifies or otherwise makes the information irretrievable.

**Policy versus Law**

As an information security professional, you must be aware of the legal environment in which your organization operates, and of how information security is maintained by means of policy.

The key difference between policy and law is that ignorance is an acceptable defense, and therefore policies must be:

- Distributed to all individuals who are expected to comply with them
- Readily available for employee reference
- Easily understood, with multilingual translations and translations for visually impaired or low-literacy employees
- Acknowledged by the employee, usually by means of a signed consent form.

## 2.4 Ethical Concepts in Information Security

**Q4. Explain in detail the legal, ethical & professional issues during the security investigation?**

*Ans :*

The student of information security is not expected to study the topic of ethics in a vacuum, but within a larger ethical framework.

However, those employed in the area of information security may be expected to be more articulate about the topic than others in the organization, and often must withstand a higher degree of scrutiny.

The Ten Commandments of Computer Ethics - from The Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

**Differences in Ethical Concepts**

- Studies reveal that individuals of different nationalities have different perspectives on the ethics of computer use.
- Difficulties arise when one nationality's ethical behavior does not correspond to that of another national group.

**Ethics and Education**

- Differences in computer use ethics are not exclusively cultural.
- Differences are found among individuals within the same country, within the same social class, and within the same company.
- Key studies reveal that the overriding factor in leveling the ethical perceptions within a small population is education.
- Employees must be trained and kept up to date on information security topics, including the expected behaviors of an ethical employee.

**Deterring Unethical and Illegal Behavior**

It is the responsibility of information security personnel to do everything in their power to deter unethical and illegal acts, using policy, education and training, and technology as controls or safeguards to protect the information and systems.

Many security professionals understand technological means of protection, but many underestimate the value of policy.

There are three general categories of unethical behavior that organizations and society should seek to eliminate:

- Ignorance
- Accident
- Intent

Deterrence is the best method for preventing an illegal or unethical activity. Laws, policies, and technical controls are all examples of deterrents. However, it is generally agreed that laws and policies and their associated penalties only deter if three conditions are present:

- Fear of penalty:
- Probability of being caught:.
- Probability of penalty being administered

### 2.4.1 Certifications and Professional Organizations

- A number of professional organizations have established codes of conduct and/or codes of ethics that members are expected to follow.
- Codes of ethics can have a positive effect on an individual's judgment regarding computer use.
- Unfortunately, many employers do not encourage their employees to join these professional organizations.

- It remains the individual responsibility of security professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society.

**Association of Computing Machinery (ACM)**

- The ACM (www.acm.org) is a respected professional society, originally established in 1947, as "the world's first educational and scientific computing society." It is one of the few organizations that strongly promotes education, and provides discounted membership for students.
- The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional.

**International Information Systems Security Certification Consortium, Inc. (ISC)2**

The (ISC)2 manages a body of knowledge on information security and administers and evaluates examinations for information security certifications.

- Currently the (ISC)2 offers two professional certifications in the information security arena: the Certification for Information Systems Security Professionals (CISSP), and the Systems Security Certified Professional, or SSCP
- The code of ethics put forth by (ISC)2 is primarily designed for information security professionals who have earned one of their certifications.
- This code includes four mandatory canons:
- Protect society, the common wealth, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession.

**System Administration, Networking, and Security Institute (SANS)**

Founded in 1989, SANS is a professional research and education cooperative organization with currently over 156,000 security professionals, auditors, system administrators, and network administrators.

SANS certifications can be pursued independently or combined to earn the comprehensive certification called the GIAC Security Engineer (GSE). The newest GIAC certification, the Information Security Officer (GISO), is an overview certification that combines basic technical knowledge with understanding of threats, risks, and best practices.

**Information Systems Audit and Control Association (ISACA)**

- The Information Systems Audit and Control Association, or ISACA (www.isaca.org), is a professional association with a focus on auditing, control, and security.
- The membership comprises both technical and managerial professionals.
- The ISACA also has a code of ethics for its professionals.
- It requires many of the same high standards for ethical performance as the other organizations and certifications.

**CSI - Computer Security Institute (CSI)**

- The Computer Security Institute (www. gocsi. com) provides information and certification to support the computer, networking, and information security professional.
- CSI also publishes a newsletter and threat advisory, and is well known for its annual computer crime survey of threats developed in cooperation with the FBI.

**Information Systems Security Association**

- The Information Systems Security Association (ISSA) (www.issa.org) is a nonprofit society of information security professionals.
- As a professional association, its primary mission is to bring together qualified practitioners of

information security for information exchange and educational development. ISSA provides conferences, meetings, publications, and information resources to promote information security awareness and education.

- ISSA also promotes a code of ethics, similar to those of (ISC)2, ISACA, and the ACM, "promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources."

**Other Security Organizations**

The Internet Society or ISOC (www.isoc.org) is a nonprofit, nongovernmental, international professional organization. It promotes the development and implementation of education, standards, policy, and education and training to promote the Internet.

The Internet Engineering Task Force (IETF) consists of individuals from the computing, networking, and telecommunications industries, and is responsible for developing the Internet's technical foundations.

Standards developed by the IETF are then reviewed by the Internet Engineering Steering Group (IESG), with appeal to the Internet Architecture Board, and promulgated by the Internet Society as international standards.

The Computer Security Division (CSD) of the National Institute for Standards and Technology (NIST) runs the Computer Security Resource Center (CSRC)—an essential resource for any current or aspiring information security professional.

This Web site (csrc.nist.gov) houses one of the most comprehensive sets of publicly available information on the entire suite of information security topics.

The CSD is involved in five major research areas related to information security:

1. Cryptographic standards and applications
2. Security testing
3. Security research and emerging technologies
4. Security management and guidance
5. Outreach, awareness, and education

The CERT Coordination Center, or CERT/CC (www.cert.org), is a center of Internet security expertise which is part of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

The CERT/CC studies security issues and provides publications and alerts to help educate the public to the threats facing information security.

The center also provides training and expertise in the handling of computer incidents. CERT/CC acts both as a research center and outside consultant in the areas of incident response, security practices, and programs development.

Computer Professionals for Social Responsibility (CPSR) is a public organization for technologists and anyone with a general concern about the impact of computer technology on society. CPSR promotes ethical and responsible development and use of computing, and seeks to inform public and private policy and lawmakers on this subject. It acts as an ethical watchdog for the development of ethical computing.

## 2.5 KEY U.S. FEDERAL AGENCIES

**Q5. Discuss about different U.S. security agencies that support information security?**

*Ans :*

There are a number of key U.S. federal agencies charged with the protection of U.S. information resources, and the investigation of threats to, or attacks on, these resources.

The Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC) (www.nipc. gov) was established in 1998 and serves as the U.S. government's focal point for threat assessment and the warning, investigation, and response to threats or attacks against critical U.S. infrastructures.

A key part of the NIPC's efforts to educate, train, inform, and involve the business and public sector in information security is the National InfraGard Program.

Every FBI field office has established an InfraGard chapter and collaborates with public and private organizations and the academic community to share information about attacks, vulnerabilities, and threats.

InfraGard's dominant contribution is the free exchange of information to and from the private sector in the subject areas of threats and attacks on information resources.

Another key federal agency is the National Security Agency (NSA). The NSA is the Nation's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information…. It is also one of the most important centers of foreign language analysis and research within the Government.

The NSA is responsible for signal intelligence and information system security.The NSA's Information Assurance Directorate (IAD) provides information security "solutions including the technologies, specifications and criteria, products, product configurations, tools, standards, operational doctrine and support activities needed to implement the protect, detect and report, and respond elements of cyber defense."

The U.S. Secret Service is a department within the Department of the Treasury. In addition to its well-known mission to protect key members of the U.S. government, the Secret Service is also charged with the detection and arrest of any person committing a U.S. federal offense relating to computer fraud, as well as false identification crimes.

The Patriot Act (Public Law 107-56) increased the Secret Service's role in investigating fraud and related activity in connection with computers.

The Department of Homeland Security is established with the passage of Public Law 107-296 which in part, transfers the United States Secret Service from the Department of the Treasury, to the new department effective March 1, 2003.

**Organizational Liability and the Need for Counsel**

What if an organization does not support or even encourage strong ethical conduct on the part of its employees?

- If an employee, acting with or without the authorization, performs an illegal or unethical act, causing some degree of harm, the organization can be held financially liable for that action.
- An organization increases its liability if it refuses to take measures—due care—to make sure that every employee knows what is acceptable and what is not, and the consequences of illegal or unethical actions.
- Due diligence requires that an organization make a valid and ongoing effort to protect others.

**Risk Management & Information Security Management Systems**

## 2.6 INTRODUCTION

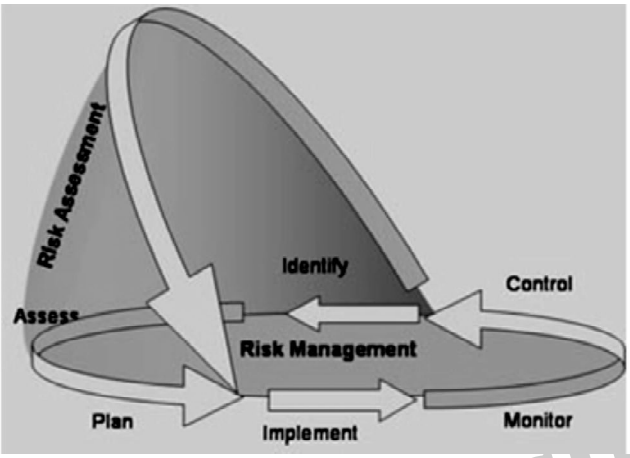
**Q6. What is Risk management? State the methods of identifying & assessing risk management?**

*Ans :*

Risk Management and Risk Assessment are major components of Information Security Management (ISM). Although they are widely known, a wide range of definitions of Risk Management and Risk Assessment are found in the relevant literature [ISO13335-2], [NIST], [ENISA Regulation]. Here a consolidated view of Risk Management and Risk Assessment is presented. For the sake of this discussion, two approaches to presenting Risk Management and Risk Assessment, mainly based on OCTAVE [OCTAVE] and ISO 13335-2 [ISO13335-2] will be considered. Nevertheless, when necessary, structural elements that emanate from other perceptions of Risk Management and Risk Assessment are also used (e.g. consideration of Risk Management and Risk Assessment as counterparts of Information Security Management System, as parts of wider operational processes, etc.

It seems to be generally accepted by Information Security experts, that Risk Assessment is part of the Risk Management process. After initialization, Risk Management is a recurrent activity

that deals with the analysis, planning, implementation, control and monitoring of implemented measurements and the enforced security policy. On the contrary, Risk Assessment is executed at discrete time points (e.g. once a year, on demand, etc.) and – until the performance of the next assessment - provides a temporary view of assessed risks and while parameterizing the entire Risk Management process. This view of the relationship of Risk Management to Risk Assessment is depicted in the following is adopted from OCTAVE .




It is worth mentioning, that in this figure both Risk Management and Risk Assessment are presented as processes, that is, as sequences of activities (s. arrows in figure above). Various standards and good practices exist for the establishment of these processes (e.g. through structuring, adaptation, re-configuration etc.). In practice, organizations tend to generate their own instantiations of these methods, in a form most suitable for a given organizational structure, business area or sector. In doing so, national or international standards (or combination of those) are taken as a basis, whereas existing security mechanisms, policies and/or infrastructure are adapted one-by-one. In this way, new *good practices* for a particular sector are created. Some representative examples of tailored methods/good practices are:

- Method based on a de facto standard (e.g. [OCTAVE]);
- A method based on a sector standard (e.g. [SIZ-DE]);
- Amethod based on a native national standard (e.g. [IT-Grund]);
- A method based on an native international standard (e.g. [ISO13335-2]);
- Amethod based on an individual basic protection profile for the IT-systems of an organization (e.g. [SIZ-PP]);
- Adoption of an already existing risk analysis of similar systems (e.g. based on an existing Protection Profiles according to Common Criteria [CC]).

In practice, combinations of the above examples are very common.

For the sake of the presentation within this site, the assumption is made, that the Risk Management life-cycle presented. (i.e. plan, implement, monitor, control, identify, assess), refers solely to risks. Similar activities that might be necessary within the Information Security Management process are considered to apply to operational aspects related to the implementation and control of security measurements.

Even although organizations tend to use a single method for Risk Management, multiple methods are typically be used in parallel for Risk Assessment. This is because different Risk Assessment methods might be necessary, depending on the nature of the assessed system (e.g. structure, criticality, complexity, importance, etc.).

Through a series of activities, ENISA has established inventories of existing Risk Management and Risk Assessment methods and tools in Europe (also referred to as *products* here). Any of these products can be used for the instantiation of both the Risk Management and Risk Assessment processes mentioned in the figure above. The contents of these inventories and the inventories themselves are presented in this site.

It should be noted that a more detailed representation of Risk Management and Risk Assessment is given in ISO 13335-2 [ISO13335-2]. In general, the contents of Risk Management and Risk Assessment processes as described here are compatible with ISO 13335. In the future, detailed examples of how to adapt the processes presented to existing business and IT-needs by means of demonstrators will be given. The generation of such material will be part future work at ENISA in form of demonstrators.

## 2.7 IT SYSTEM CHARACTERIZATION

**Q7. Explain different characteristics of IT systems that support Risk assessment report?**

*Ans :*

IT system characterization defines the scope of the risk assessment effort. Use the previously-developed IT System Inventory and Definition Document (Appendix B of the Guideline) as input for this step; some additional information is required. The purpose of this step is to identify the IT system, to define the risk assessment boundary and components, and to identify the IT system and data sensitivity

IT System IdentificationInclude in the Risk Assessment Report the previously developed IT System Inventory and Definition Document.

| IT System Inventory and Definition Document | | | |
|---|---|---|---|
| **IT System Identification and Ownership** | | | |
| **IT System ID** | BFA-001 | IT System Common Name | Budget Formulation System (BFS) |
| **Owned By** | Budget Formulation Agency (BFA)<br>Financial Operations Division (FOD) | | |
| **Physical Location** | BFA Data Center<br>123 E. Elm Street, Richmond, VA 23299 | | |
| **Major Business Function** | Enable processing of current-year budget details and future-year budget plans | | |
| **System Owner Phone Number** | John James<br>(804) 979-3757 | **System Administrator(s) Phone Number** | Partner Systems, Inc.<br>(888) 989-8989 |
| **Data Owner(s) Phone Number(s)** | Mike Williams<br>(804) 979-3452<br>Bill Michaels<br>(804) 979-3455 | **Data Custodian(s) Phone Number(s)** | Bea Roberts<br>Partner Systems, Inc.<br>(888) 989-8989 |
| **Other Relevant Information** | BFS has been in production since December 1996 | | |

| IT System Boundary and Components | |
|---|---|
| **IT System Description and Components** | BFS is a distributed client-server application transported by a network provided by PSI, a third-party. The major components of the BFS include:<br>• A Sparc SUNW, Ultra Enterprise 3500 server running SunOS 5.7 (Solaris |

| | |
|---|---|
| | 7). The server has four (4) processors running at 248 MHz, 2048 MB of memory, 4 SBus cards, 4 PCI cards, and total disk storage capacity of 368.6 GB (36 drives x 10 GB). This system is provided to BFA under contract by PSI, and this Risk Assessment relies on information regarding system hardware and Operating System software provided to BFA by PSI.<br>• One (1) network interface that is connected to BFA's data center Cisco switch. This interface is assigned two unique IP addresses.<br>• An Oracle 9i data store with two (2) commercial off-the-shelf (COTS) application modules (ABC and XYZ) purchased from Oracle Corporation. |
| **IT System Interfaces** | • An interface between BFS and the Budget Consolidation System (BCS). This interface allows only the BCS to securely transmit data using the Secure Copy Protocol (SCP) on port 22 into the BFS nightly by a cron job that refreshes tables in the BFS Oracle store with selected data from BCS tables.<br>• A modem for emergency dial-in support and diagnostics, secured via the use of a one-time password authentication mechanism.<br>• Client software located within the Agency's Windows 2003 Server Active Directory Domain to manage access to BFS. This software utilizes encrypted communications between the client and the server and connects to the server on port 1521. Only users with the appropriate rights within the BFA Domain can access the client software, although a separate client login and password is required to gain access to BFS data and functions. This access is based on Oracle roles and is granted by the BFS system administrators to users based on their job functions. |
| **IT System Boundary** | • The demarcation between the BFS and the Local Area Network (LAN) is the physical port on the Cisco switch that connects the BFS to the network. The switch and other network components are not considered to be part of the BFS.<br>• BFS support personnel provide the operation and maintenance of the application. The BFS personnel provide the operation and maintenance of the server and operating system. The BFS boundary is the following directories and their sub-subdirectories: /var/opt/Oracle, /databases/Oracle, and /opt/odbc. Other directories are outside the BFS boundary.<br>• BFS is responsible for receiving data from the BCS. The BCS is a separate system and is outside the BFS boundary.<br>• Client access to the BFS server is controlled by BFA's Windows 2003 Server Active Directory domain. This access are included within the BFS system boundary. The overall BFA Windows 2003 Server Active Directory domain, however, is not considered to be part of the BFS, and is outside the BFS boundary. |

| IT System Interconnections | | | | |
|---|---|---|---|---|
| **Agency or Organization** | **IT System Name** | **IT System ID** | **IT System Owner** | **Interconnection Security Agreement Summary** |
| BFA | Budget Consolidation System | BCS | John James | No formal agreement required, as systems have common owner |
| Partner Services, Inc. (PSI) | Enterprise Data Network | EDN | Bea Roberts | Agreement is in place; expires 12/31/2007; under renegotiation |

| IT System and Data Sensitivity | | | |
|---|---|---|---|
| **Type of Data** | **Sensitivity Ratings Include Rationale for each Rating** | | |
| | **Confidentiality** | **Integrity** | **Availability** |
| **Current Year Budget Details** | Low<br>Data is public information | High<br>BFS is system of record for fiscal year budget data for all COV Agencies | Moderate<br>Data is used less than daily by all COV Agencies to allocate resources |
| **Future Year Budge Plans** | High<br>Release of the data before it is final could be damaging to COV and its Agencies | Moderate<br>BFS is system of record for future year budget plans for all COV Agencies | Low/High<br>Low during most of year; high during budget preparation |
| **Overall IT System Sensitivity Rating and Classification** | Overall IT System Sensitivity Rating<br>Must be "high" if sensitivity of any data type is rated "high" on any criterion | | |
| | HIGH | MODERATE | LOW |
| | IT System Classification Must be "Sensitive" if overall sensitivity is "high"; consider as "Sensitive" if overall sensitivity is "moderate" | | |
| | SENSITIVE | | NON-SENSITIVE |

## 2.8 RISK IDENTIFICATION

**Q8. Explain asset identification & valuation of Risk?**

*Ans :*

The purpose of this step is to identify the risks to the IT system. Risks occur in IT systems when vulnerabilities (i.e., flaws or weaknesses) in the IT system or its environment can be exploited by threats. The process of risk identification consists of three components:

1. Identification of vulnerabilities in the IT system and its environment;
2. Identification of credible threats that could affect the IT system; and
3. Pairing of vulnerabilities with credible threats to identify risks to which the IT system is exposed.

After the process of risk identification is complete, likelihood and impact of risks will be considered.

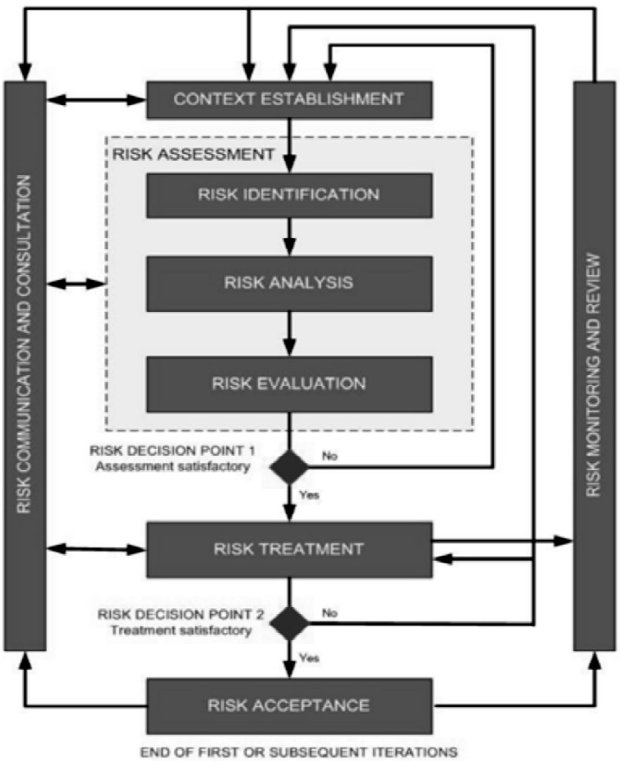
### Risk Identification

The first component of risk identification is to identify vulnerabilities in the IT system and its environment. There are many methodologies or frameworks for determining IT system vulnerabilities. The methodology should be selected based on the phase of the IT system is in its life cycle. For an IT system:

- In the Project Initiation Phase, the search for vulnerabilities should focus on the organizations IT security policies, planned procedures and IT system requirements definition, and the vendor's security product analyses (e.g., white papers).
- In the Project Definition Phase, the identification of vulnerabilities should be expanded to include more specific information. Assess the effectiveness of the planned IT security features described in the security and system design documentation.

In the Implementation Phase, the identification of vulnerabilities should also include an analysis of the security features and the technical and procedural security controls used to protect the system. These evaluations include activities such as executing a security self-assessment, the effective application of automated vulnerability scanning/assessment tools and/or conducting a third-party penetration test. Often, a mixture of these and other methods is used to get a more comprehensive list of vulnerabilities.

Include in the Risk Assessment Report a description of how vulnerabilities were determined. If a Risk Assessment has been performed previously, it should contain a list of vulnerabilities that should be assessed to determine their continued validity. In addition, assess and document if any new vulnerabilities exist.



### Identification of Credible Threats

The purpose of this component of risk identification is to identify the credible threats to the IT system and its environment. A threat is credible if it has the potential to exploit an identified vulnerability.

Table at the end of this section, contains examples of threats. The threats listed in the table are provided only as an example and are specific to the example BFS system. Agencies are encouraged to consult other threat information sources, such as NIST SP 800-30. The goal is to identify all credible threats to the IT system, but not to create a universal list of general threats.

Include in the Risk Assessment Report a description of how threats were determined. If a Risk Assessment has been performed previously, it should contain a list of credible threats that must be assessed to determine their continued validity. In addition, assess and document if any new vulnerabilities exist.

Include a brief description of how credible threats were determined and a list of the credible threats in the Risk Assessment Report.

| Credible Threats Identified | | |
|---|---|---|
| Air Conditioning Failure | Earthquakes | Nuclear Accidents |
| Aircraft Accident | Electromagnetic Interference | Pandemic |
| Biological Contamination | Fire (Major or Minor) | Power Loss |
| Blackmail | Flooding/Water Damage | Sabotage |
| Bomb Threats | Fraud/Embezzlement | Terrorism |
| Chemical Spills | Hardware Failure | Tornados, Hurricanes, Blizzards |
| Communication Failure | Human Error | Unauthorized Access or Use |
| Computer Crime | Loss of Key Personnel | Vandalism and/or Rioting |
| Cyber-Terrorism | Malicious Use | Workplace Violence |



## 2.9 Identification of Risks

**Q9. What is risk management? What is the identification of risk by listing assets & vulnerabilities is so important in the risk management process?**

*Ans :*

The final component of risk identification is to pair identified vulnerabilities with credible threats that could exploit them and expose the following to significant risk:

- IT system;
- The data it handles; and
- The organization.

In order to focus risk management efforts on those risks that are likely to materialize, it is important both to be comprehensive in developing the list of risks to the IT system and also to limit the list to pairs of actual vulnerabilities and credible threats. For example, as noted at the beginning of section 3, Oracle 9i

will stop responding when sent a counterfeit packet larger than 50,000 bytes. This flaw constitutes vulnerability. A malicious user or computer criminal might exploit this vulnerability to stop an IT system from functioning. This possibility constitutes a threat. This vulnerability-threat pair combines to create a risk that an IT system could become unavailable.

If an IT system running Oracle 9i is not connected to a network, however, such as the certificate authority for a Public Key Infrastructure (PKI) system, then there is no credible threat, and so no vulnerability-threat pair to create a risk.

Provide a brief description of how the risks were identified, and prepare a table of all risks specific to this IT system. In the table, each vulnerability should be paired with at least one appropriate threat, and a corresponding risk. The risks should be numbered and each risk should include a description of the results if the vulnerability was to be exploited by the threat.

| Vulnerabilities, Threats, and Risks | | | | |
|---|---|---|---|---|
| **Risk No.** | **Vulnerability** | **Threat** | **Risk of Compromise of** | **Risk Summary** |
| 1 | Wet-pipe sprinkler system in BFS Data Center. | Fire | Availability of BFS and data. | Fire would activate sprinkler System causing water damage & compro-mising the availabil-ity of BFS. |
| 2 | BFS user identifiers (IDs) no longer required are not removed from BFS in timely manner. | Unauthorized Use | Confidentiality & integrity of BFS data. | Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of BFS data. |
| 3 | BFS access privileges are granted on an ad-hoc basis rather than using predefined roles. | Unauthorized Access | Confidentiality & integrity of BFS data. | Unauthorized access via ad-hoc privileges could compromise of confidentiality & integrity of BFS data. |
| 4 | Bogus TCP packets (> 50000 bytes) directed at port 1521 will cause BFS to stop responding. | Malicious Use Computer Crime | Availability of BFS and data. | Denial of service attack via large bogus packets sent to port 1521 could render BFS unavailable for use. |
| 5 | New patches to correct flaws in application security design have not been applied. | Malicious Use Computer Crime | Confidentiality & integrity of BFS data. | Exploitation of un-patched application security flaws could compromise confidentiality & integrity of BFS data. |
| 6 | User names & passwords are in scripts & initialization files. | Malicious Use Computer Crime | Con-fi-dentiality & integrity of BFS data. | Exploitation of passwords in script & initialization files could result in compromise of con-fi-dentiality & integrity of BFS data. |
| 7 | Passwords are not set to expire; regular password changes are not enforced. | Malicious Use Computer Crime | Confiden-tial-ity & integrity of BFS data. | Compromise of unexpired/unchanged passwords could result in compromise of confiden-tial-ity & integrity of BFS data. |
| 8 | "Generic" accounts found in the database (e.g., test, share, guest). | Malicious Use Computer Crime | Confidentiality & integrity of BFS data. | Use of generic BFS accounts could result in compromise of confidentiality & integrity of sensitive BFS data. |
| 9 | Remote OS authentication is enabled but not used. | Malicious Use Computer Crime | Confidentiality & integrity of BFS data. | Remote access is not currently used by BFS; enabling this access when not necessary could result in compromise of confidentiality & integrity of Sensitive BFS data. |
| 10 | Login encryption setting is not properly configured. | Malicious Use Computer Crime | Confidentiality & integrity of BFS data. | Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive BFS data. |
| 11 | Sensitive BFS data is stored on USB drives | Malicious Use Computer Crime | Confidentiality of BFS data. | Loss or theft of USB drives could result in compromise of confidentiality of BFS data. |

## 2.10 Risk Control Analysis

**Q10. Explain in detail different roles & Responsibilities of Risk Analysis?**

*Ans :*

The purpose of this step is to document a list of security controls used for the IT system. These controls should correspond to the requirements of the Policy, Standard, and Audit Standard. The analysis should also specify whether the control is in-place (i.e., current) or planned, and whether the control is currently enforced. In the next step these controls are matched with the risks identified. in order to identify those risks that require additional response. a security controls list that corresponds to the requirements of the Policy, Standard, and Audit Standard. This list shows controls that are in-place, as well as those planned for implementation.

**IT Security Roles & Responsibilities**

Required IT Security roles have been assigned in writing, both for BFA as a whole, & for the BFS. John Howard, BFA Commissioner, has designated Jane Jones as BFA ISO & delegated the assignment of other IT security roles to her.

With respect to BFS, Jane Jones has assigned individuals to the required IT security roles, as documented elsewhere in this report.

- **Business Impact Analysis:**

  BFA management & staff conducted & documented a Business Impact Analysis (BIA) of the Agency during June 2004; this BIA was updated in May 2007. The BFA BIA notes that the BFS supports essential BFA functions.

- **IT System & Data Sensitivity Classi- fication:**

  BFA has documented classification of the sensitivity of BFA IT systems & data, including the BFS. This classification notes the high sensitivity of much of the data handled by the BFS.

- **IT System Inventory & Definition:**

  BFA has documented an inventory of its sensitive IT systems; this inventory includes the BFS; the System Definition of BFS is included in Section 2 of this Risk Assessment report.

**Risk Assessment**

- This report documents the Risk Assessment of BFS in July 2007, building on an earlier BFS Risk Assessment in July 2004.
- BFA will validate the current Risk Assessment through annual self-assessments in July 2008 & July 2009, & will conduct the next formal BFS RA in July 2010, or sooner, if necessary.

**IT Security Audits**

- Anne Keller, BFA Internal Audit Director manages IT Security Audits for BFA.
- An IT Security Audit of BFS was conducted & documented by BFA Internal Audit staff on June 24, 2007.
- Required reporting for the BFS CAP is in place.
- Future IT Security Audits of BFA are planned biennially.

**Continuity of Operations Planning**

- Sam Robinson is the BFA Continuity of Operations Plan (COOP) Coordinator & also serves as the focal point for IT COOP & Disaster Recovery (DR) activities.
- The BFA COOP documents the requirements for 24-hour recovery of the BFS & its data to support budget preparation, & 72-hour recovery of BFS & its data at other times.
- The BFA COOP identifies all personnel required for its execution, including personnel required for recovery of the BFS, & includes emergency declaration, notification, & operations procedures.
- The COOP document is classified as sensitive; access to this document is restricted to COOP team members, & a copy of the COOP is stored off site at Data Recovery Services, Inc., BFA's recovery site partner.
- Recovery procedures for BFS were most recently tested during BFA's annual COOP exercise on May 18-20, 2007.
- The BFA COOP, including components relating to the BFS is currently being updated as a result of the COOP exercise; completion is expected by September 1, 2007.
- Recovery procedures for BFS will next be tested during the BFA COOP exercise scheduled for May 2008.

| Control Area | In-Place/ Planned | Description of Controls |
|---|---|---|
| IT Systems Interoperability Security | In place | The BFS receives data only from the BCS; it does not transmit data to any other IT system. This data sharing is documentedof this Risk Assessment, & in the BCS Risk Assessment. John James is System Owner of both BCS & BFS; therefore no written data sharing agreement is required. Security of network access is covered by a documented interoperability security agreement between John James, BFS System Owner, & Bea Roberts, System Owner of the PSI third-party network. |
| Malicious Code Protection | In place | BFA has two different anti-virus software products installed on its desktop & laptop computers & on its e-mail servers. This software:<br>Eliminates or quarantines all malicious programs that it detects & provides an alert to the user upon detection;<br>Runs automatically on power-on & runs weekly full scans on memory & storage devices;<br>Automatically scans all files retrieved from all sources;<br>Allows only system administrators to modify its configuration; &Maintains a log of protection activities;<br>Eliminates or quarantines malicious programs in e-mail messages & file attachments as they attempt to enter the Agency's e-mail system.<br>Both desktop/laptop & e-mail anti-virus software are configured for automatic download of definition files whenever new files become available. |
| | Planned | The BFA Acceptable Use Policy, under development, will prohibit BFA users from intentionally developing or experimenting with malicious programs & knowingly propagating malicious programs including opening attachments from unknown sources. This policy is scheduled for completion in August 2007. |
| IT Systems Development Life Cycle Security | In place | The BFS is in the Implementation phase of its life cycle. As documented throughout this Risk Assessment report, BFA conducts & documents a formal Risk Assessment of the BFS every three years. In addition the BFS complies with all other Risk Management requirements of the COV IT Security Standard. |

| | | |
|---|---|---|
| Account Management | In place | Documented BFA & BFS policies require:<br>Granting access to IT system users based on the principle of least privilege. In the case of BFS, however, enforcement of least privilege is accomplished by granting ad-hoc access rights to BFS, rather than granting access based on pre-defined roles.<br>Approval by John James, BFS System Owner & a prospective BFS user's supervisor before granting access to BFS; these policies are enforced.<br>Prospective BFS users to receive a BFA-required criminal background check before receiving access to BFS; these policies are enforced.<br>The use of passwords on all BFS accounts, & that these passwords expire every 90 days, at a minimum. These policies are not enforced on BFS, however, as pass-words are not set to expire & password changes are not enforced.<br>Annual review of all BFS accounts to assess the continued need for the accounts & access level. These policies also require automatic locking of accounts if not used for 30 days, disabling of unneeded accounts, retention of account information for 2 years in accordance with BFA records retention policy, & notification of supervisors, Human Resources, & the System Administrator about changes in the need for BFS accounts. These policies are not enforced on BFS, however, & BFS user accounts are not removed when the access is no longer required.<br>Prohibit the use of group accounts & shared passwords. These policies are not enforced on BFS, however, as accounts such as "guest," "test," & "share" exist in the BFS user database.<br>John James to approve access changes to BFS accounts,& for John James & the BFS operations & support team to investigate unusual account access. These policies are enforced. |

| | | |
|---|---|---|
| Password Management | In place | Documented BFA & BFS policies require:<br>The use of passwords on sensitive systems such as BFS; these policies are enforced on BFS. These policies also require that, at a minimum, passwords be no less than eight characters long & contain both letters & numbers; Windows Active Directory is configured to require this length & complexity for BFS passwords.<br>Encryption of passwords during transmission; password encryption, however, is not correctly configured for BFS & BFS passwords are transmitted in clear text.<br>Users to maintain exclusive control of their passwords, to allow users to change their passwords at will, & to change a password immediately & notify the ISO if the password is compromised; these policies are enforced.<br>BFS users to change passwords every 90 days at a minimum; as noted above, however, these policies are not enforced with respect to BFS.<br>The use of password history files to present password re-use; these policies are enforced on BFS & BFS retains the previous 240 passwords for each user to prevent their re-use.<br>**Documented BFA & BFS policies require:**<br>• Use of a procedure for delivery of the initial BFS password in person from the BFS support team in a sealed envelope. The password is expired, & the user is forced to change the password upon first login. Forgotten initial passwords are replaced by the BFS support team & not re-issued.<br>• Prohibit the use of group accounts & shared passwords. These policies are not enforced on BFS, however, as accounts such as "guest," "test," & "share" exist in the BFS user database.<br>• Prohibit the inclusion of passwords as plain text in scripts. These policies are not enforced on BFS, however, as passwords are included in scripts & initialization files.<br>• Limit access to files containing BFS passwords to the BFS support team. These policies are enforced.<br>• Suppression of passwords on the screen as they are entered. These policies are enforced.<br>• Members of the BFS support team to have both an administrative & user account & use the administrative account only when performing tasks that require administrative privileges. These policies are enforced.<br>• At least two members of the BFS support team to have BFS administrative account. |
| Remote Access | In place | 1. Based on the sensitivity of BFS data, documented BFA & BFS policies require that remote access to BFS not be permitted from outside the PSI-provided third-party network. Remote OS authentication, however, is enabled in the BFS application, even though no user accounts are configured to allow this access. |

To enable alternate work schedules, & work locations, BFA is in the process of

| | | |
|---|---|---|
| | Planned | 2. To enable alternate work schedules, & work locations, BFA is in the process of developing a plan to allow secure remote access to BFS. This plan is scheduled for completion in October 2007. |
| Data Storage Media Protection | In place | Documented BFA & BFS policies require:<br>• Bea Roberts, as BFS Data Custodian, to provide protection of all sensitive BFS data. These requirements are enforced a written agreement between BFA &Partner Services, Inc.<br>• Sensitive BFS data not to be stored on mobile data storage media through BFA policy that prohibits local storage of BFS data. This policy is not enforced, however, as sensitive BFS data is stored on USB drives.<br>• Only authorized DRSI personnel to pickup, receive, transfer, & deliver BFS tapes. This policy is enforced.<br>• BFS administrators & users to follow the ITRM Removal of Commonwealth Data from Surplus Computer Hard Drives & Electronic Media Standard (ITRM Standard SEC2003-02.1) when disposing of BFS data storage media that are no longer needed. This policy is enforced.<br>• BFS users to receive training on the proper procedure for disposal of data storage media containing sensitive data as part of the BFA IT Security Awareness & Training program. This policy is enforced. |

## 2.11 Risk Control Strategies

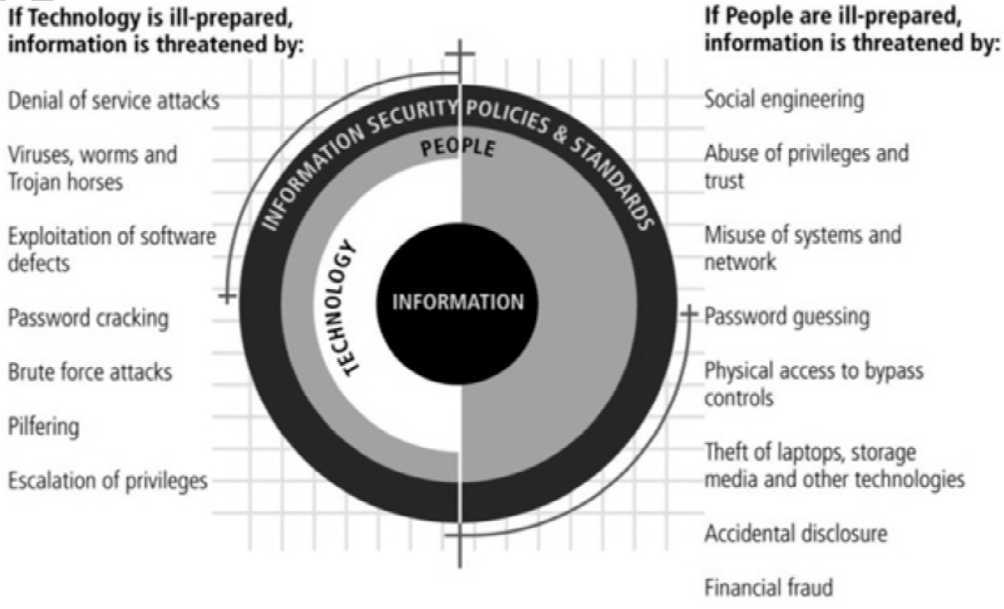
**Q11. Explain in detail different Risk control strategies?**

*Ans :*

An organization must choose one of four basic strategies to control risks:

1. **Avoidance:** applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability
2. **Transference:** shifting the risk to other areas or to outside entities
3. **Mitigation:** reducing the impact should the vulnerability be exploited
4. **Acceptance:** understanding the consequences and accept the risk without control or mitigation





### Avoidance

Avoidance is the risk control strategy that attempts to prevent the exploitation of the vulnerability.

Avoidance is accomplished through:

- Application of policy
- Application of training and education
- Countering threats
- Implementation of technical security controls and safeguards

### Transference

Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations.

This may be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or by implementing service contracts with providers.

### Mitigation

Mitigation is the control approach that attempts to reduce, by means of planning and preparation, the damage caused by the exploitation of vulnerability.

This approach includes three types of plans:

- the disaster recovery plan (DRP),
- incident response plan (IRP), and
- business continuity plan (BCP).

Mitigation depends upon the ability to detect and respond to an attack as quickly as possible.

| Plan | Description | Example | When deployed | Timeframe |
|---|---|---|---|---|
| Incident Response Plan (IRP) | Actions an organization takes during incidents (attacks) | ▪ List of steps to be taken during disaster<br>▪ Intelligence gathering<br>▪ Information analysis | As incident or disaster unfolds | Immediate and real-time reaction |
| Disaster Recovery Plan (DRP) | ▪ Preparations for recovery should a disaster occur<br>▪ Strategies to limit losses before and during disaster<br>▪ Step-by-step instructions to regain normalcy | ▪ Procedures for the recovery of lost data<br>▪ Procedures for the reestablishment of lost services<br>▪ Shutdown procedures to protect systems and data | Immediately after the incident is labeled a disaster | Short-term recovery |
| Business Continuity Plan (BCP) | Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DRP's ability to quickly restore operations | ▪ Preparation steps for activation of secondary data centers<br>▪ Establishment of a hot site in a remote location | Immediately after the disaster is determined to affect the continued operations of the organization | Long-term operation |

### Acceptance

As described above, mitigation is a control approach that attempts to reduce the impact of an exploited vulnerability.

In contrast, acceptance of risk is the choice to do nothing to protect an information asset and to accept the outcome from any resulting exploitation.

This control, or lack of control, assumes that it may be a prudent business decision to examine the alternatives and conclude that the cost of protecting an asset does not justify the security expenditure.

The only valid use of the acceptance strategy occurs when the organization has:

- Determined the level of risk to the information asset
- Assessed the probability of attack and the likelihood of a successful exploitation of a vulnerability
- Approximated the ARO of the exploit
- Estimated the potential loss from attacks
- Performed a thorough cost benefit analysis
- Evaluated controls using each appropriate type of feasibility
- Decided that the particular asset did not justify the cost of protection

## 2.12 Risk Control Strategy Selection

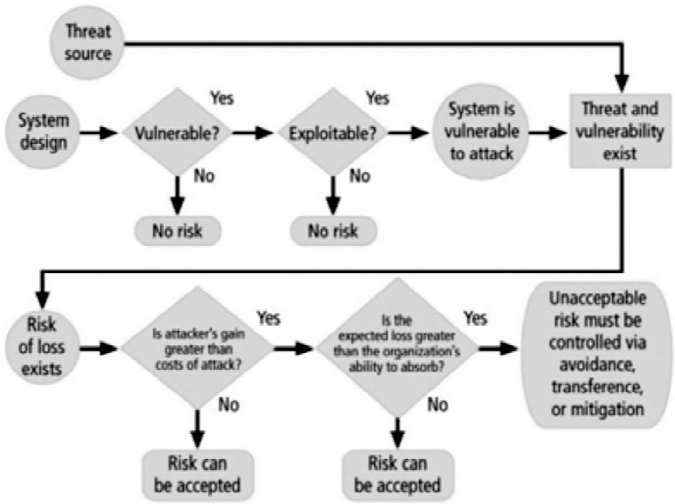
**Q12. Explain in detail the process of asset identification of different Strategies of selecting & Controling Risk?**

*Ans :*

Risk control involves selecting one of the four risk control strategies for the vulnerabilities present within the organization.

If the loss is within the range of losses the organization can absorb, or if the attacker's gain is less than expected costs of the attack, the organization may choose to accept the risk.

Otherwise, one of the other control strategies will have to be selected.

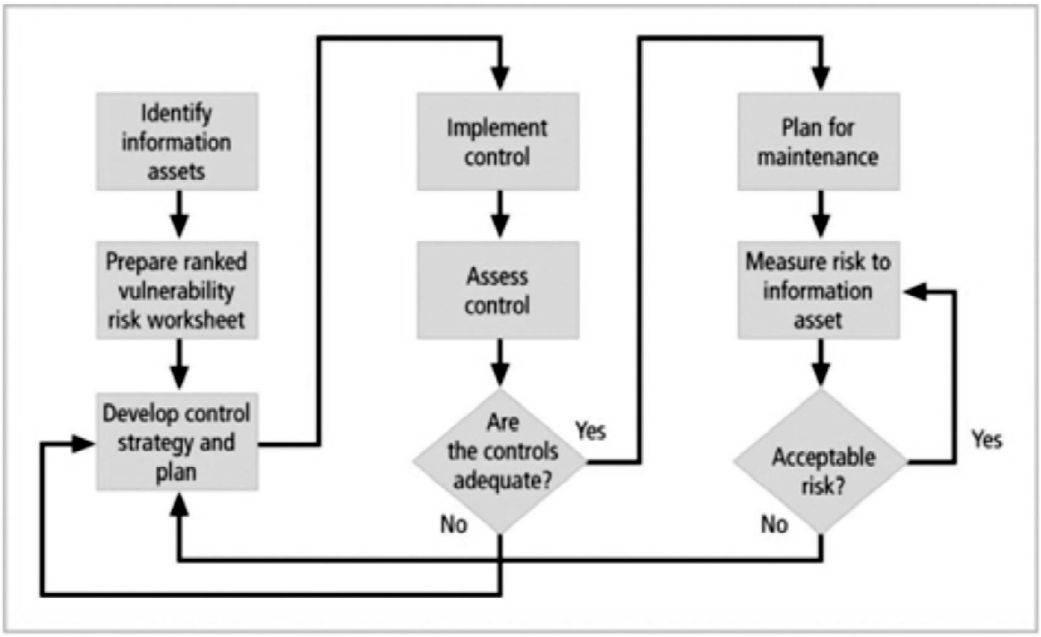


**Some rules of thumb on strategy selection are:**

- When a vulnerability exists: Implement security controls to reduce the likelihood of a vulnerability being exercised.
- When a vulnerability can be exploited: Apply layered controls to minimize the risk or prevent occurrence.
- When the attacker's potential gain is greater than the costs of attack: Apply protections to increase the attacker's cost, or reduce the attacker's gain, using technical or managerial controls.
- When potential loss is substantial: Apply design controls to limit the extent of the attack, thereby reducing the potential for loss.

**Evaluation, Assessment, and Maintenance of Risk Controls**

Once a control strategy has been selected and implemented, the effectiveness of controls should be monitored and measured on an ongoing basis to determine its effectiveness and the accuracy of the estimate of the risk that will remain after all planned controls are in place.



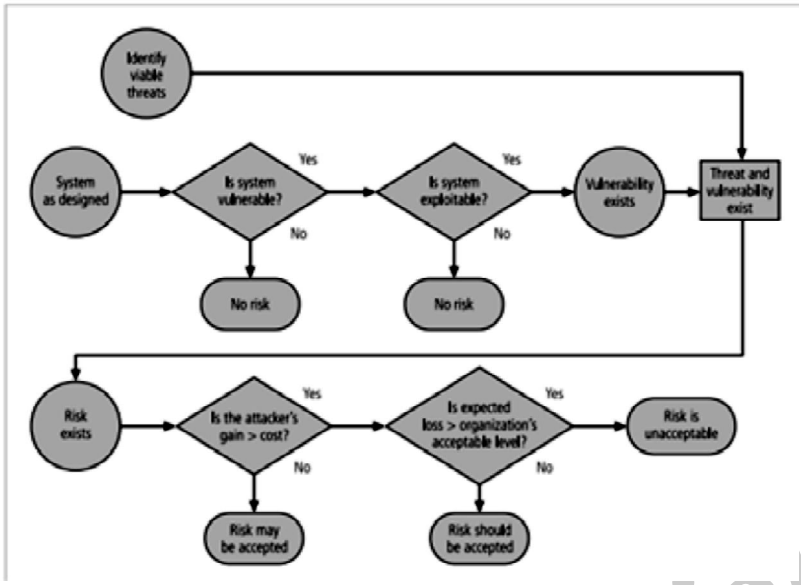

**Feasibility Studies and Cost Benefit Analysis**

Before deciding on the strategy for a specific vulnerability, all readily accessible information about the consequences of the vulnerability must be explored.

"What are the advantages of implementing a control as opposed to the disadvantages of implementing the control?"

There are a number of ways to determine the advantage or disadvantage of a specific control.

The primary means is to determine the value of the information assets that it is designed to protect.




**Cost Benefit Analysis (CBA)**

The criterion most commonly used when evaluating a project that implements information security controls and safeguards is economic feasibility.

Organizations are urged to begin a cost benefit analysis by evaluating the worth of the information assets to be protected and the loss in value if those information assets are compromised by the exploitation of a specific vulnerability.

This decision-making process is called a cost benefit analysis or an economic feasibility study.

**Cost**

Just as it is difficult to determine the value of information, it is difficult to determine the cost of safeguarding it.

**Some of the items that affect the cost of a control or safeguard include:**

- Cost of development or acquisition of hardware, software, and services
- Training fees
- Cost of implementation
- Service costs
- Cost of maintenance

**Benefit**

Benefit is the value to the organization of using controls to prevent losses associated with a specific vulnerability.

The benefit is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk and how much risk there is for the asset.

This is expressed as the annualized loss expectancy (ALE).

**Asset Valuation**

Asset valuation is the process of assigning financial value or worth to each information asset.

The value of information differs within organizations and between organizations, based on the characteristics of information and the perceived value of that information.

The valuation of assets involves estimation of real and perceived costs associated with the design, development, installation, maintenance, protection, recovery, and defense against loss and litigation.

Some of the components of asset valuation include:

- Value retained from the cost of creating the information asset
- Value retained from past maintenance of the information asset
- Value implied by the cost of replacing the information
- Value from providing the information
- Value acquired from the cost of protecting the information
- Value to owners
- Value of intellectual property
- Value to adversaries
- Loss of productivity while the information assets are unavailable
- Loss of revenue while information assets are unavailable

An organization must be able to place a dollar value on each collection of information and the information assets it owns, based on:

- How much did it cost to create or acquire this information?
- How much would it cost to recreate or recover this information?
- How much does it cost to maintain this information?
- How much is this information worth to the organization?
- How much is this information worth to the competition?

Next the organization examines the potential loss that could occur from the exploitation of vulnerability or a threat occurrence. This process results in the estimate of potential loss per risk.

The questions that must be asked here include:

- What damage could occur, and what financial impact would it have?
- What would it cost to recover from the attack, in addition to the financial impact of damage?
- What is the single loss expectancy for each risk?

A single loss expectancy, or SLE, is the calculation of the value associated with the most likely loss from an attack.

It is a calculation based on the value of the asset and the expected percentage of loss that would occur from a particular attack:

**SLE = asset value (AV) x exposure factor (EF)**

Where EF = the percentage loss that would occur from a given vulnerability being exploited.This information is usually estimated.

In most cases, the probability of a threat occurring is usually a loosely derived table indicating the probability of an attack from each threat type within a given time frame.

This value is commonly referred to as the ARO, or annualized rate of occurrence.

- In order to standardize calculations, you convert the rate to a yearly (annualized) value.

- This is expressed as the probability of a threat occurrence.
- Once each asset's worth is known, the next step is to ascertain how much loss is expected from a single attack, and how often these attacks occur.
- Once those values are determined, the equation can be completed to determine the overall lost potential per risk.

This is usually determined via an annualized loss expectancy, or ALE, using the values for the ARO and SLE from previous sections.

**ALE = SLE x ARO**

**The Cost Benefit Analysis (CBA) Formula**

CBA determines whether or not a control alternative is worth its associated cost.

CBAs may be calculated before a control or safeguard is implemented, to determine if the control is worth implementing, or calculated after controls have been implemented and have been functioning for a time.

**CBA = ALE(prior) – ALE(post) – ACS**

ALE(prior to control) is the annualized loss expectancy of the risk before the implementation of the control.

ALE(post control) is the ALE examined after the control has been in place for a period of time. ACS is the annual cost of the safeguard.

**Other Feasibility Studies**

In the previous sections the concepts of economic feasibility or using baselines or benchmarks were used to justify proposals for information security controls.

The next step in measuring how ready an organization is for these controls is determining the proposal's organizational, operational, technical, and political feasibility.

Organizational feasibility analysis examines how well the proposed information security alternatives will contribute to the operation of an organization.

Operational feasibility addresses user acceptance and support, management acceptance and support, and the overall requirements of the organization's stakeholders.

Technical feasibility examines whether or not the organization has or can acquire the technology to implement and support the alternatives.

Political feasibility defines what can and cannot occur based on the consensus and relationships between the communities of interest.

**Benchmarking**

Benchmarking is the process of seeking out and studying the practices used in other organizations that produce the results you desire in your organization.

An organization typically benchmarks by selecting a measure with which to compare itself with the other organizations in its market.

The organization then measures the difference in the way it conducts business and the way the other organizations conduct business.

When benchmarking, an organization typically uses one of two measures to compare practices: metrics-based measures or process-based measures.

Metrics-based measures are comparisons based on numerical standards, such as:

- Numbers of successful attacks
- Staff hours spent on systems protection
- Dollars spent on protection
- Numbers of security personnel
- Estimated value in dollars of the information lost in successful attacks
- Loss in productivity hours associated with successful attacks

Process-based measures are generally less focused on numbers and are more strategic.

For each of the areas the organization is interested in benchmarking, process based measures enable the companies to examine the activities an individual company performs in pursuit of its goal, rather than the specifics of how goals are attained.

The primary focus is the method the organization uses to accomplish a particular process, rather than the outcome.

In the field of information security, two categories of benchmarks are used :

- standards of due care and due diligence, and
- best practices.

Within best practices, the gold standard is a subcategory of practices that are typically viewed as "the best of the best."

### Due Care and Due Diligence

For legal reasons, an organization may be forced to adopt a certain minimum level of security.

When organizations adopt levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances. This is referred to as a standard of due care.

Due diligence is the demonstration that the organization is persistent in ensuring that the implemented standards continue to provide the required level of protection.

### Best Business Practices.

Security efforts that seek to provide a superior level of performance are referred to as best business practices.

Best security practices are those that are among the best in the industry, balancing access to information with adequate protection, while maintaining a solid degree of fiscal responsibility.

Companies with best practices may not be the best in every area, but may simply have established an extremely high quality or successful security effort in one or more area.

### The Gold Standard

Even the best business practices are not sufficient for some organizations. These organizations aspire to set the standard by implementing the most protective, supportive, and yet fiscally responsible standards they can.

The gold standard is a defining level of performance that demonstrates a company's industrial leadership, quality, and concern for the protection of information.

Seeking the gold standard is a method of striving for excellence.

### Applying Best Practices

When considering best practices for adoption, address the following questions:

- Does your organization resemble the organization that is implementing the best practice under consideration?
- Is your organization in a similar industry?
- Does your organization face similar challenges?
- Is your organizational structure similar to the organization from which you are modeling the best practices?
- Can your organization expend resources that are in line with the requirements of the best practice?
- Is your organization in a similar threat environment as the one cited in the best practice?

### Problems with Benchmarking and Best Practices

- Organizations don't talk to each other.
- No two organizations are identical.
- Best practices are a moving target.
- Simply knowing what was going on a few years ago, doesn't necessarily indicate what to do next.

### Baselining

Baselining is the analysis of measures against established standards.

In information security, baselining is the comparison of security activities and events against the organization's future performance.

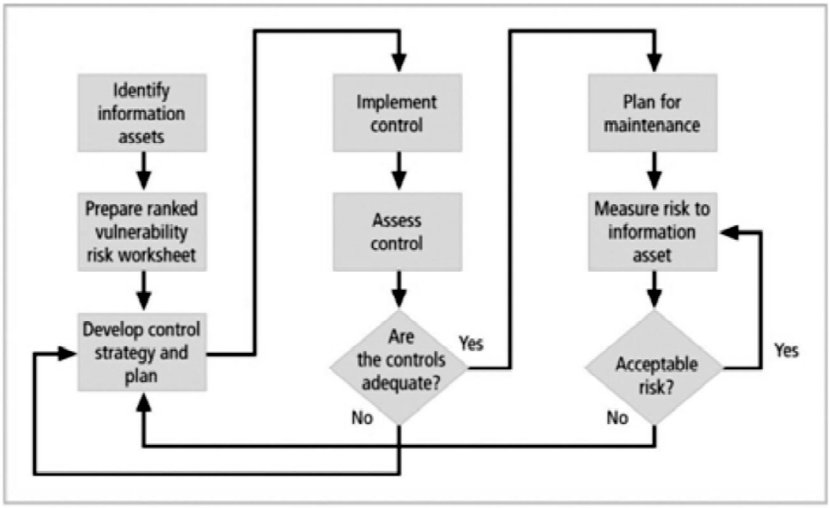
The information gathered for an organization's first risk assessment becomes the baseline for future comparisons.

## 2.13 Quantitative Vs Qualitative Risk Control Practices

**Q13. Explain the relation b/w Qualitative & Quantative Analysis of Risk Management?**

*Ans :*

The many steps described previously were performed using actual values or estimates. This is known as a quantitative assessment. However, an organization could decide that it cannot put specific numbers on these values. Fortunately, it is possible to repeat these steps using an evaluation process, called qualitative assessment, that does not use numerical measures. For example, instead of placing a value of once every 10 years for the ARO, the organization could list all possible attacks on a particular set of information and rate each by the probability of occurrence. This could be accomplished using scales rather than specific estimates. A sample scale could include none, representing no chance of occurrence, then low, medium, high, up to very high, representing almost certain occurrence. Organizations may, of course, prefer other scales: A–Z, 0–10, 1–5, or 0–20. Using scales also relieves the organization from the difficulty of determining exact values. Many of these same scales can be used in any situation requiring a value, even in asset valuation. For example, instead of estimating that a particular piece of information is worth $1 million, you can value information on a scale of 1–20, with 1 indicating relatively worthless information, and 20 indicating extremely critical information, such as a certain soda manufacturer's secret recipe or those eleven herbs and spices of a popular fried chicken vendor.




Benchmarking and Best Practices Instead of determining the financial value of information and then implementing security as an acceptable percentage of that value, an organization could take a different approach to risk management and look to peer organizations for benchmarks. Benchmarking is the process of seeking out and studying the practices used in other organizations that produce results you would like to duplicate in your organization. An organization typically benchmarks itself against other institutions by selecting a measure upon which to base the comparison. The organization then measures the difference between the way it conducts business and the way the other organizations conduct business. The industry Web site Best Practices Online puts it this way: Benchmarking can yield great benefits in the education of executives and the realized performance improvements of operations. In addition, benchmarking can be used to determine strategic areas of opportunity. In general, it is the application of what is learned in benchmarking that delivers the marked and impressive results so often noted. The determination of benchmarks allows one to make a direct comparison. Any identified gaps are improvement areas.

When benchmarking, an organization typically uses one of two types of measures to compare practices: metrics-based measures or process-based measures.

Metrics-based measures are comparisons based on numerical standards, such as:

- Numbers of successful attacks
- Staff-hours spent on systems protection
- Dollars spent on protection
- Numbers of security personnel
- Estimated value in dollars of the information lost in successful attacks
- Loss in productivity hours associated with successful attacks

An organization uses numerical standards like these to rank competing organizations with a similar size or market to its own and then determines how it measures up to the competitors. The difference between an organization's measures and those of others is often referred to as a performance gap. Performance gaps provide insight into the areas that an organization should work on to improve its security postures and defenses.

The other measures commonly used in benchmarking are process-based measures. Process-based measures are generally less focused on numbers and are more strategic than metrics-based measures. For each of the areas the organization is interested in benchmarking, process-based measures enable the organization to examine the activities an individual company performs in pursuit of its goal, rather than the specifics of how goals are attained. The primary focus is the method the organization uses to accomplish a particular process, rather than the outcome. In information security, two categories of benchmarks are used: standards of due care and due diligence, and best practices.

For legal reasons, an organization may be forced to adopt a certain minimum level of security, as discussed. When organizations adopt levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances. This is referred to as a standard of due care. It is insufficient to implement these standards and then ignore them. The application of controls at or above the prescribed levels and the maintenance of those standards of due care show that the organization has performed due diligence. Due diligence is the demonstration that the organization is diligent in ensuring that the implemented standards continue to provide the required level of protection. Failure to maintain a standard of due care or due diligence can open an organization to legal liability, provided it can be shown that the organization was negligent in its application or lack of application of information protection. This is especially important in areas in which the organization maintains information about customers, including medical, legal, or other personal data.

The security an organization is expected to maintain is complex and broad in scope. It may, therefore, be physically impossible to be the "best in class" in any or all categories. Based on the budgets assigned to the protection of information, it may also be financially impossible to provide a level of security equal to organizations with greater revenues. Sometimes organizations want to implement the best, most technologically advanced, most secure levels of protection, but for financial or other reasons they cannot. Such organizations should remember the adage, "Good security now is better than perfect security never." It would also be counterproductive to establish costly, state-of-the-art security in one area, only to leave other areas exposed. Organizations must make sure they have met a reasonable level of security across the board, protecting all information, before beginning to improve individual areas to reach a higher standard, such as best practices.

### Applying Best Practices

The preceding sections have presented a number of sources you can consider when applying standards to your organization. You can study the documented best practice processes or procedures that have been shown to be effective and are thus recommended by a person or organization and evaluate how they apply to your organization. When considering best practices for adoption, consider the following:

- Does your organization resemble the identified target organization with the best practice under consideration? Is your organization in a similar industry as the target? Keep in mind that a strategy that works well in manufacturing organizations often has little bearing in a nonprofit organization. Does your organization face similar challenges as the target? If your organization has no functioning information security program, a best practice target that assumes you start with a functioning program is not useful. Is your organizational structure similar to the target's? Obviously, a best practice proposed for a small home office setting is not appropriate for a multinational company.
- Are the resources your organization can expend similar to those identified with the best practice? If your approach is significantly limited by resources, it is not useful to submit a best practice proposal that assumes unlimited funding.
- Is your organization in a similar threat environment as that proposed in the best practice? A best practice from months and even weeks ago may not be appropriate for the current threat environment. Think of the best practices for Internet connectivity that are required in the modern organization at the opening of the 21st century and compare them to the best practices of 5 years earlier.

Another source for best practices information is the CERT Web site (www.cert.org/nav/ index_ green.html), which presents a number of articles and practices. Similarly, Microsoft publishes its security practices on its Web site (www. microsoft. com/security/default.mspx).

Microsoft focuses on the following seven key areas for home users:

1. Use antivirus software.
2. Use strong passwords.
3. Verify your software security settings.
4. Update product security.
5. Build personal firewalls.
6. Back up early and often.
7. Protect against power surges and loss.

For the small businesses Microsoft recommends the following:

**1. Protect desktops and laptops**

Keep software up to date, protect against viruses, and set up a firewall.

**2. Keep data safe**

Implement a regular backup procedure to safeguard critical business data, set permissions, and use encryption.

**3. Use the Internet safely**

Unscrupulous Web sites, popups, and animations can be dangerous. Set rules about Internet usage.

**4. Protect the network**

Remote network access is a security risk you should closely monitor. Use strong passwords and be especially cautious about wireless networks.

**5. Protect servers**

Servers are the network's command center-protect your servers.

**6. Secure business applications**

Make sure that software critical to your business operations is fully secure around the clock.

**7. Manage desktops and laptops from the server**

Without stringent administrative procedures in place, security measures may be unintentionally jeopardized by users.

## 2.14 Risk Management Discussion Points

**Q14. What are the different documents of requirements to solving Risk Management?**

*Ans :*

**Risk Appetite**

Risk appetite defines the quantity and nature of risk that organizations are willing to accept, as they evaluate the trade-offs between perfect security and unlimited accessibility.

The reasoned approach to risk is one that balances the expense against the possible losses if exploited.

**Residual Risk**

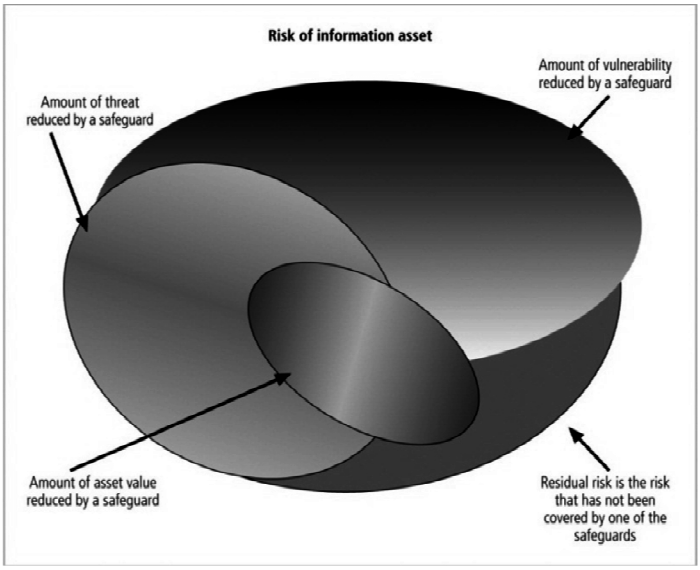
When vulnerabilities have been controlled as much as possible, there is often remaining risk that has not been completely removed, shifted, or planned for. This remainder is called residual risk.

"Residual Risk is a combined function of

(1) A threat less the effect of threat-reducing safeguards;

(2) A vulnerability less the effect of vulnerability-reducing safeguards,

(3) An asset less the effect of asset value-reducing safeguards."




The significance of residual risk must be judged within the context of an organization.The goal of information security is not to bring residual risk to zero, but to bring it in line with an organization's risk appetite.

If decision makers have been informed of uncontrolled risks and the proper authority groups within the communities of interest decide to leave residual risk in place, then the information security program has accomplished its primary goal.

**Documenting Results**

When the risk management program of an organization has been completed, the result is that a series of proposed controls are prepared, each of which is justified by one or more feasibility or rationalization approaches.

At a minimum, each information asset-threat pair should have a documented control strategy that clearly identifies any residual risk remaining after the proposed strategy has been executed.

Some organizations document the outcome of the control strategy for each information asset-threat pair in an action plan that includes concrete tasks, each with accountability assigned to an organizational unit or to an individual.

## 2.15 RECOMMENDATIONS

**Q15. Explain about OCTAVE method of Controling Risks?**

*Ans :*

The purpose of this step is to recommend additional actions required to respond to the identified risks, as appropriate to the agency's operations. The goal of the recommended risk response is to reduce the residual risk to the system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

**Recommended Risk Control Practices**

**Qualitative Measures**

- Quantitative assessment performs asset valuation with actual values or estimates.
- An organization could determine that it cannot put specific numbers on these values.
- Organizations could use qualitative assessments instead, using scales instead of specific estimates.

**The OCTAVE Method**

The Operationally Critical Threat, Asset, and Vulnerability Evaluation(OCTAVE) Method defines the essential components of a comprehensive, systematic,context-driven, self-directed information-security risk evaluation.

By following the OCTAVE Method, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information technology assets. The operational or business units and the IT department work together to address the information security needs of the organization.

- **Phase 1:** Build Asset-Based Threat Profiles – This is an organizational evaluation.Key areas of expertise within the organization are examined to elicit important knowledge about information assets, the threats to those assets, the security requirements of the assets, what the organization is currently doing to protect its information assets and weaknesses in organizational policies and practice.
- **Phase 2:** Identify Infrastructure Vulnera bilities – This is an evaluation of the information infrastructure. The key operational components of the information technology infrastructure are examined for weaknesses (technology vulnerabilities) that can lead to unauthorized action.
- **Phase 3:** Develop Security Strategy and Plans – Risks are analyzed in this phase. The information generated by the organizational and information infrastructure evaluations (Phases 1 and 2) is analyzed to identify risks to the organization and to evaluate the risks based on their impact to the organization's mission.

In addition, an organization protection strategy and risk mitigation plans for the highest priority risks are developed.

**Important Aspects of the OCTAVE Method**

- The OCTAVE Method is self directed.
- The OCTAVE Method requires an analysis team to conduct the evaluation and to analyze the information. The basic tasks of the team are:
  - to facilitate the knowledge elicitation workshops of Phase 1
  - to gather any supporting data that are necessary
  - to analyze threat and risk information
  - to develop a protection strategy for the organization
  - to develop mitigation plans to address the risks to the organization's critical assets

- The OCTAVE Method uses a workshop-based approach for gathering information and making decisions.
- The OCTAVE Method relies upon the following major catalogs of information:
- catalog of practices – a collection of good strategic and operational security practices
- threat profile – the range of major sources of threats that an organization needs to consider
- catalog of vulnerabilities – a collection of vulnerabilities based on platform and application

**Phases, Processes and Activities**

Each phase of the OCTAVE Method contains two or more processes. Each process is made of activities.

**Phase 1:** Build Asset-Based Threat Profiles

- **Process 1:** Identify Senior Management Knowledge
- **Process 2:** Identify Operational Area Management Knowledge
- **Process 3:** Identify Staff Knowledge
- **Process 4:** Create Threat Profiles

**Phase 2:** Identify Infrastructure Vulnerabilities

- **Process 5:** Identify Key Components
- **Process 6:** Evaluate Selected Components

**Phase 3:** Develop Security Strategy and Plans

- **Process 7:** Conduct Risk Analysis
- **Process 8:** Develop Protection Strategy

**Preparing For the OCTAVE Method**

- Obtain senior management sponsorship of OCTAVE.
- Select analysis team members.
- Train analysis team.
- Select operational areas to participate in OCTAVE.
- Select participants.
- Coordinate logistics.
- Brief all participants.

UNIT III

**Planning for Security:** Security policy, Standards and practices, Security blue print, Security education, Continuity strategies.

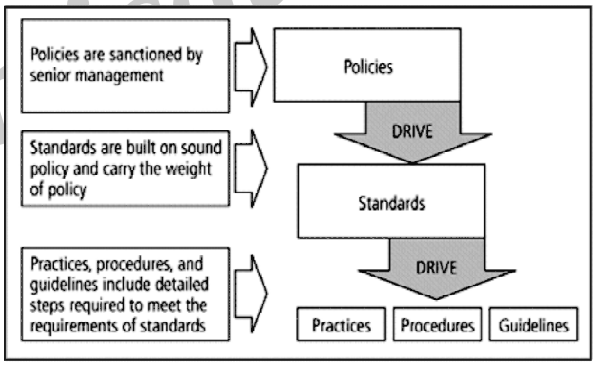
**Security Technology:** Firewalls and VPNs, Physical design, Firewalls, Protecting remote connections

## 3.1 Introduction to Policy

**Q1. Why Policy ? What are its approaches?**

*Ans :*

- A quality information security program begins and ends with policy
- Policies are least expensive means of control and often the most difficult to implement
- Some basic rules must be followed when shaping a policy :
  - Never conflict with law
  - Stand up in court
  - Properly supported and administered
  - Contribute to the success of the organization
  - Involve end users of information systems.
- **Policy** : course of action used by an organization to convey instructions from management to those who perform duties
- Organizational rules for acceptable/ unacceptable behavior
- Penalties for violations
- Appeals process
- **Standards**: more detailed statements of what must be done to comply with policy
- **Practices, procedures and guidelines** effectively explain how to comply with policy
- For a policy to be effective it must be
  - Properly disseminated
  - Read
  - Understood
  - Agreed to by all members of organization.




**Types of Policies**

- Enterprise information Security program Policy(EISP)
- Issue-specific information Security Policy ( ISSP)
- Systems-specific information Security Policy (SYSSP)

For a policy to be effective and thus legally enforceable, it must meet the following criteria :

1. **Dissemination (distribution)—**The organization must be able to demonstrate that the policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.

2. **Review (reading)—**The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees. Common techniques include recording the policy in English and other languages.
3. **Comprehension (understanding)—**The organization must be able to demonstrate that the employee understood the requirements and content of the policy. Common techniques include quizzes and other assessments.
4. **Compliance (agreement) -** The organization must be able to demonstrate that the employee agrees to comply with the policy, through act or affirmation. Common techniques include logon banners which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.
5. **Uniform enforcement—**The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

**Enterprise Information Security Policy (EISP)**

- Also Known as a general Security policy, IT security policy, or information security policy.
- Sets strategic direction, scope, and tone for all security efforts within the organization
- Assigns responsibilities to various areas of information security
- Guides development, implementation, and management of information security program

**Issue-Specific Security Policy (ISSP)**

**The ISSP :**

- Addresses specific areas of technology
- Requires frequent updates
- Contains statement on position on specific issue

**Approaches to creating and managing ISSPs :**

- Create number of independent ISSP documents
- Create a single comprehensive ISSP document
- Create a modular ISSP document

**ISSP topics could include :**

- E-mail, use of Web, configurations of computers to defend against worms and viruses, prohibitions against hacking or testing organisation security controls, home use of company-owned computer equipment, use of personal equipment on company networks, use of telecommunications technologies(FAX and phone), use of photocopiers

**Components of the ISSP**

1. **Statement of Policy**
   - Scope and Applicability
   - Definition of Technology Addressed
   - Responsibilities
2. **Authorized Access and Usage of Equipment**
   - User Access
   - Fair and Responsible Use
   - Protection of Privacy
3. **Prohibited Usage of Equipment**
   - Disruptive Use or Misuse
   - Criminal Use
   - Offensive or Harassing Materials
   - Copyrighted, Licensed or other Intellectual Property
   - Other Restrictions
4. **Systems Management**
   - Management of Stored Materials
   - Employer Monitoring
   - Virus Protection
   - Physical Security
   - Encryption

**5. Violations of Policy**

- Procedures for Reporting Violations
- Penalties for Violations

**6. Policy Review and Modification**

- Scheduled Review of Policy and Procedures for Modification

**7. Limitations of Liability**

- Statements of Liability or Disclaimers

**Systems-Specific Policy (SysSP)**

- SysSPs are frequently codified as standards and procedures to be used when configuring or maintaining systems
- Systems-specific policies fall into two groups:
- **Access control lists (ACLs)** consist of the access control lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system
- **Configuration rules** comprise the specific configuration codes entered into security systems to guide the execution of the system

**ACL Policies**

- Both Microsoft Windows NT/2000 and Novell Netware 5.x/6.x families of systems translate ACLs into sets of configurations that administrators use to control access to their respective systems
- ACLs allow a configuration to restrict access from anyone and anywhere

**ACLs regulate:**

- Who can use the system
- What authorized users can access
- When authorized users can access the system
- Where authorized users can access the system from
- How authorized users can access the system

**The Information Security Blueprint**

- It is the basis for the design, selection, and implementation of all security policies, education and training programs, and technological controls.
- More detailed version of **security framework**, which is an outline of overall information security strategy for organization and a road map for planned changes to the information security environment of the organization.
- Should specify tasks to be accomplished and the order in which they are to be realized.
- Should also serve as a scalable, upgradeable, and comprehensive plan for the information security needs for coming years.

## 3.2 SECURITY MODELS/SECURITY STANDARDS AND PRACTICES

**Q2. What are ISO17799 and BS 7799? Explain different sections & Sailent features?**

*Ans :*

**ISO 17799/BS 7799**

- One of the most widely referenced and often discussed security models is the Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799
- In 2000, this Code of Practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799.

**Drawbacks of ISO 17799/BS 7799**

- Several countries have not adopted 17799 claiming there are fundamental problems:
  - The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
  - 17799 lacks "the necessary measurement precision of a technical standard"
  - There is no reason to believe that 17799 is more useful than any other approach currently available.

- 17799 is not as complete as other frameworks available
- 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls

**Objectives of ISO 17799**

Organizational Security Policy is needed to provide management direction and support.

**Ten Sections of ISO/IEC 17799**

a) Organizational Security Policy

b) Organizational Security Infrastructure

c) Asset Classification and Control

d) Personnel Security

e) Physical and Environmental Security

f) Communications and Operations Management

g) System Access Control

h) System Development and Maintenance

i) Business Continuity Planning

j) Compliance

**Alternate Security Models available other than ISO 17799/BS 7799**

**NIST Security Models**

- This refers to "The National Security Telecommunications and Information systems Security Committee" document. This document presents a comprehensive model for information security. The model consists of three dimensions.
- Another possible approach available is described in the many documents available from the Computer Security Resource Center of the National Institute for Standards and Technology (csrc.nist.gov).

The following NIST documents can assist in the design of a security framework:

- **NIST SP 800-12 :** An Introduction to Computer Security: The NIST Handbook
- **NIST SP 800-14 :** Generally Accepted Security Principles and Practices for Securing IT Systems
- **NIST SP 800-18** : The Guide for Developing Security Plans for IT Systems
- **NIST SP 800-26**: Security Self-Assessment Guide for IT systems.
- **NIST SP 800-30**: Risk Management for IT systems.

**NIST Special Publication SP 800-12**

- **SP 800-12** is an excellent reference and guide for the security manager or administrator in the routine management of information security.
- It provides little guidance, however, on design and implementation of new security systems, and therefore should be used only as a valuable precursor to understanding an information security blueprint.

**NIST Special Publication SP 800-14**

- Generally accepted Principles and practices for Security Information Technology Systems.
- Provides best practices and security principles that can direct the security team in the development of **Security Blue Print**.
- The scope of NIST SP 800-14 is broad. It is important to consider each of the security principles it presents, and therefore the following sections examine some of the more significant points in more detail :
  - Security Supports the Mission of the Organization
  - Security is an Integral Element of Sound Management
  - Security Should Be Cost-Effective
  - Systems Owners Have Security Responsibilities Outside Their Own Organizations
  - Security Responsibilities and Accountability Should Be Made Explicit
  - Security Requires a Comprehensive and Integrated Approach
  - Security Should Be Periodically Reassessed

- Security is Constrained by Societal Factors
- 33 Principles enumerated

### 3.2.1 NIST SP 800-18

**Q3. Explain the sailent features NIST security models?**

*Ans :*

- The Guide for Developing Security plans for Information Technology Systems can be used as the foundation for a comprehensive security blueprint and framework.
- It provides detailed methods for assessing, and implementing controls and plans for applications of varying size.
- It can serve as a useful guide to the activities and as an aid in the planning process.
- It also includes templates for major application security plans.
- The table of contents for Publication 800-18 is presented in the following.

**System Analysis**

- System Boundaries
- Multiple similar systems
- System Categories

**Plan Development- All Systems**

- Plan control
- System identification
- System Operational status
- System Interconnection/ Information Sharing
- Sensitivity of information handled
- Laws, regulations and policies affecting the system

**Management Controls**

- Risk Assessment and Management
- Review of Security Controls
- Rules of behavior
- Planning for security in the life cycle
- Authorization of Processing (Certification and Accreditation)
- System Security Plan

**Operational Controls**

1. Personnel Security
2. Physical Security
3. Production, Input/Output Controls
4. Contingency Planning
5. Hardware and Systems Software
6. Data Integrity
7. Documentation
8. Security Awareness, Training, and Education
9. Incident Response Capability

**Technical Controls**

- Identification and Authentication
- Logical Access Controls
- Audit Trails

**NIST SP 800-26**

Security Self-Assessment Guide for IT systems.

**NIST SP 800-26 Table of contents**

**Management Controls**

1. Risk Management
2. Review of Security Controls
3. Life Cycle Maintenance
4. Authorization of Processing (Certification and Accreditation)
5. System Security Plan

**Operational Controls**

1. Personnel Security
2. Physical Security
3. Production, Input/Output Controls
4. Contingency Planning
5. Hardware and Systems Software
6. Data Integrity
7. Documentation

8. Security Awareness, Training, and Education
9. Incident Response Capability

**Technical Controls**

1. Identification and Authentication
2. Logical Access Controls
3. Audit Trails

**Management controls** address the design and implementation of the security planning process and security program management. They also address risk management and security control reviews. They further describe the necessity and scope of legal compliance and the maintenance of the entire security life cycle.

**Operational controls** deal with the operational functionality of security in the organization. They include management functions and lower level planning, such as disaster recovery and incident response planning. They also address personnel security, physical security, and the protection of production inputs and outputs. They guide the development of education, training and awareness programs for users, administrators, and management. Finally, they address hardware and software systems maintenance and the integrity of data.

**Technical controls** address the tactical and technical issues related to designing and implementing security in the organization, as well as issues related to examining and selecting the technologies appropriate to protecting information. They address the specifics of technology selection and the acquisition of certain technical components. They also include logical access controls, such as identification, authentication, authorization, and accountability. They cover cryptography to protect information in storage and transit. Finally, they include the classification of assets and users, to facilitate the authorization levels needed.

Using the three sets of controls, the organization should be able to specify controls to cover the entire spectrum of safeguards, from strategic to tactical, and from managerial to technical.

### 3.2.2 VISA International Security Model

**Q4. Explain about VISA security model in detail?**

*Ans :*

- It promotes strong security measures in its business associates and has established guidelines for the security of its information systems.
- It has developed two important documents
  - Security Assessment Process
  - Agreed Upon Procedures.
- Both documents provide specific instructions on the use of the VISA Cardholder Information Security Program.
- The Security Assessment Process document is a series of recommendations for the detailed examination of an organization's systems with the eventual goal of integration into the VISA systems.
- The Agreed upon Procedures document outlines the policies and technologies required for security systems that carry the sensitive card holder information to and from VISA systems.
- Using the two documents, a security team can develop a sound strategy for the design of good security architecture.
- The only downside to this approach is the specific focus on systems that can or do integrate with VISA's systems with the explicit purpose of carrying the aforementioned cardholder information.

**Baselining & Best Business Practices**

- Baselining and best practices are solid methods for collecting security practices, but provide less detail than a complete methodology
- Possible to gain information by baselining and using best practices and thus work backwards to an effective design

- The Federal Agency Security Practices (FASP) site (fasp.nist.gov) designed to provide best practices for public agencies and adapted easily to private institutions.
- The documents found in this site include specific examples of key policies and planning documents, implementation strategies for key technologies, and position descriptions for key security personnel.
- Of particular value is the section on program management, which includes the following:
  - A summary guide: public law, executive orders, and policy documents
  - Position description for computer system security officer.
  - Position description for information security officer
  - Position description for computer specialist.
  - Sample of an information technology (IT) security staffing plan for a large service application(LSA)
  - Sample of an information technology (IT) security program policy
  - Security handbook and standard operating procedures.
  - Telecommuting and mobile computer security policy.

## 3.3 Security Blue Print

**Q5. What is information security Blue Print? Explain its sailent features.**

*Ans :*

Once an organization has developed its information security policies and standards, the information security community can begin developing the blueprint for the information security program. If one or more components of policies, standards, or practices have not been completed, management must determine whether or not to nonetheless proceed with the development of the blueprint.

After the information security team has inventoried the organization's information assets and assessed and prioritized the threats to those assets, it must conduct a series of risk assessments using quantitative or qualitative analyses, as well as feasibility studies and cost benefit analyses. These assessments, which include determining each asset's current protection level, are used to decide whether or not to proceed with any given control.

Armed with a general idea of the vulnerabilities in the information technology systems of the organization, the security team develops a design blueprint for security, which is used to implement the security program.

This security blueprint is the basis for the design, selection, and implementation of all security program elements including policy implementation, ongoing policy management, risk management programs, education and training programs, technological controls, and maintenance of the security program.

The security blueprint, built on top of the organization's information security policies, is a scalable, upgradeable, comprehensive plan to meet the organization's current and future information security needs. It is a detailed version of the security framework, which is an outline of the overall information security strategy for the organization and a roadmap for planned changes to the information security environment of the organization. The blueprint specifies the tasks and the order in which they are to be accomplished.

To select a methodology in which to develop an information security blueprint, you can adapt or adopt a published information security model or framework. This framework can outline steps to take to design and implement information security in the organization.There are a number of published information security frameworks,including ones from government sources, which are presented later in this chapter. Because each information security environment is unique, the security team may need to modify or adapt pieces from several frameworks. Experience teaches you that what works well for one organization may not precisely fit another.

| | |
|---|---|
| 1. | Risk Assessment and Treatment |
| 2. | Security Policy |
| 3. | Organization of Information Security |
| 4. | Asset Management |
| 5. | Human Resource Security |
| 6. | Physical and Environmental Security |
| 7. | Communications and Operations |
| 8. | Access Control |
| 9. | Information Systems Acquisition, Development and Maintenance |
| 10. | Information Security Incident Management |
| 11. | Business Continuity Management |
| 12. | Compliance |

**The ISO 27000 Series**

One of the most widely referenced security models is the Information Technology—Code of Practice for Information Security Management, which was originally published as British Standard BS7799. In 2000, this code of practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) as ISO/IEC 17799. The document was revised in 2005 (becoming ISO 17799:2005), and it was then renamed to ISO 27002 in 2007, to align it with the document ISO 27001, discussed later in this chapter. While the details of ISO/IEC 27002 are available to those who purchase the standard, its structure and general organization are well known.

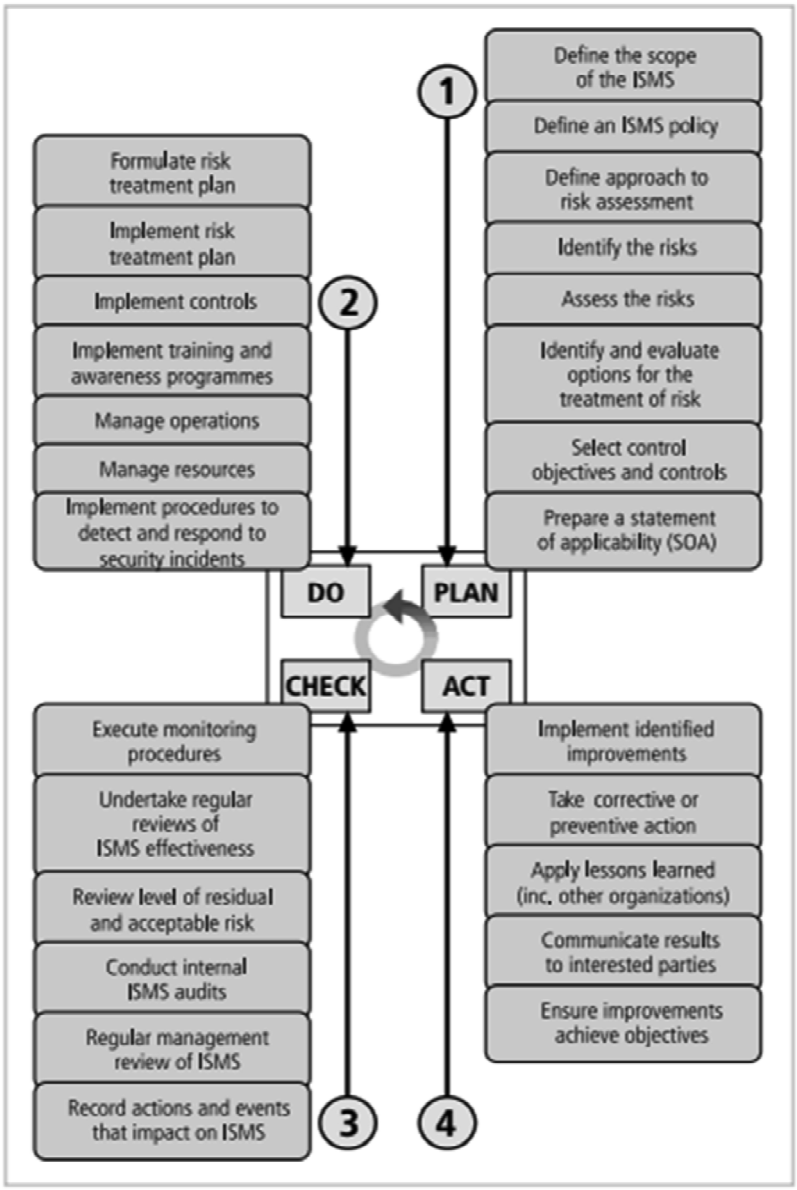
The stated purpose of ISO/IEC 27002 is to "give recommendations for information security management for use by those who are responsible for initiating, implementing, or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings."11 Where ISO/IEC 27002 is focused on a broad overview of the various areas of security, providing information on 127 controls over ten broad areas, ISO/IEC 27001 provides information on how to implement ISO/IEC 27002 and how to set up an information security management system (ISMS).

In the United Kingdom, correct implementation of these standards (both volumes), as determined by a BS7799 certified evaluator, allowed organizations to obtain information security management system (ISMS) certification and accreditation. When the standard first came out, several countries, including the United States, Germany, and Japan, refused to adopted it, claiming that there were fundamental problems, including:

- The global information security community had not defined any justification for a code of practice as identified in the ISO/IEC 17799.

- ISO/IEC 17799 lacked "the necessary measurement precision of a technical standard."
- There was no reason to believe that ISO/IEC 17799 was more useful than any other approach.
- ISO/IEC 17799 was not as complete as other frameworks.
- ISO/IEC 17799 was hurriedly prepared given the tremendous impact its adoption could have on industry information security controls.

ISO/IEC 27002 is an interesting framework for information security, but aside from those relatively few U.S. organizations that operate in the European Union (or are otherwise obliged to meet its terms), most U.S. organizations are not expected to comply with it.



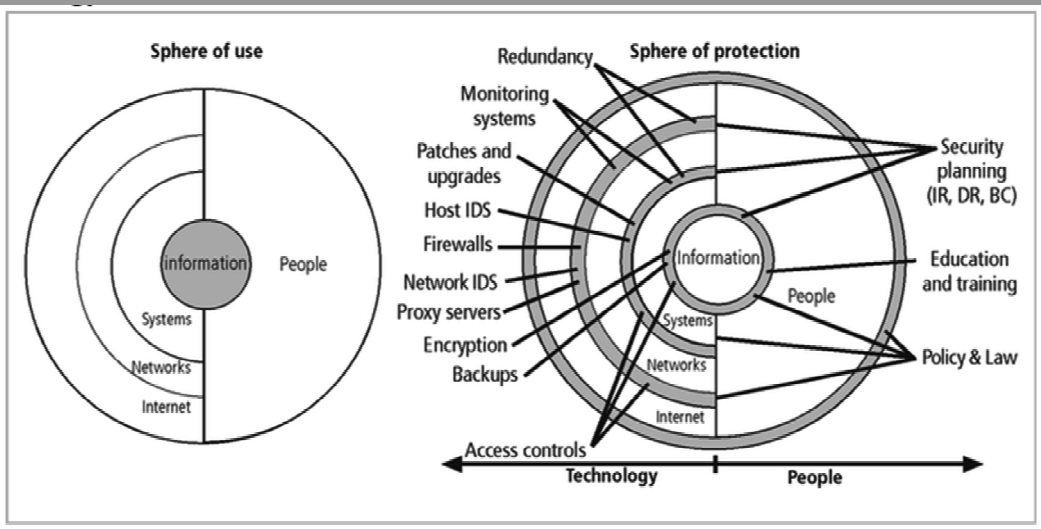
### 3.3.1 Hybrid Framework for a Blueprint of an Information Security System

The framework of security includes philosophical components of the Human Firewall Project, which maintain that people, not technology, are the primary defenders of information assets in an information security program, and are uniquely responsible for their protection.

- The spheres of security are the foundation of the security framework.
- The sphere of use, at the left in fig, explains the ways in which people access information; for example, people read hard copies of documents and can also access information through systems.
- The sphere of protection at the right illustrates that between each layer of the sphere of use there must exist a layer of protection to prevent access to the inner layer from the outer layer.
- Each shaded band is a layer of protection and control.

**Sphere of Protection**

- The "sphere of protection" overlays each of the levels of the "sphere of use" with a layer of security, protecting that layer from direct or indirect use through the next layer
- The people must become a layer of security, a **human firewall** that protects the information from unauthorized access and use
- Information security is therefore designed and implemented in three layers
  - Policies
  - People (education, training, and awareness programs)
  - Technology




- As illustrated in the sphere of protection, a variety of controls can be used to protect the information.
- The items of control shown in the figure are not intended to be comprehensive but rather illustrate individual safeguards that can protect the various systems that are located closer to the center of the sphere.
- However, because people can directly access each ring as well as the information at the core of the model, the side of the sphere of protection that attempt to control access by relying on people requires a different approach to security than the side that uses technology.

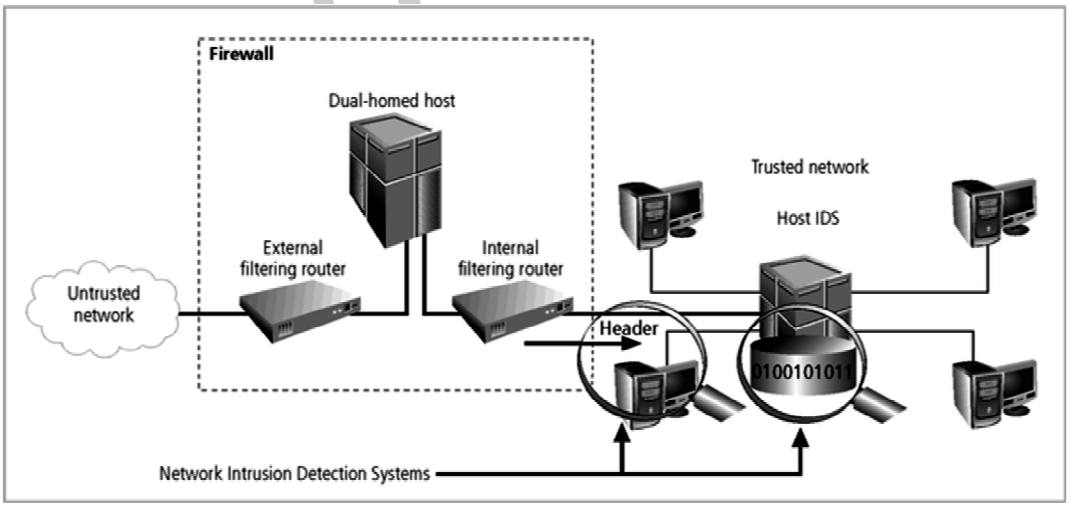
## 3.4 Design of Security Architecture

**Q6. Explain with diagram the design of Security Architecture?**

*Ans :*

### Defense in Depth

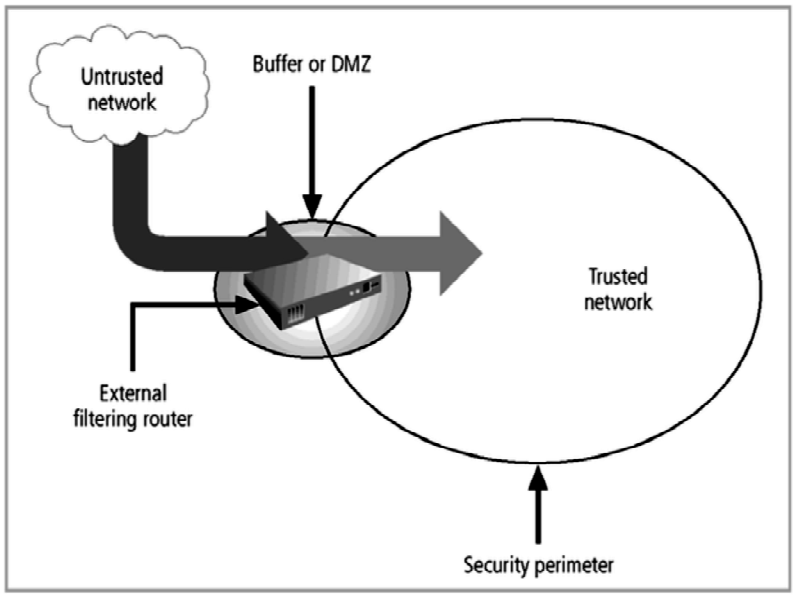
- One of the basic foundations of security architectures is the implementation of security in layers. This layered approach is called defense in depth.
- Defense in depth requires that the organization establish sufficient security controls and safeguards, so that an intruder faces multiple layers of controls.
- These layers of control can be organized into policy, training and education and technology as per the NSTISSC model.
- While policy itself may not prevent attacks, they coupled with other layers and deter attacks.
- Training and Education are similar.
- Technology is also implemented in layers, with detection equipment, all operating behind access control mechanisms.
- Implementing multiple types of technology and thereby preventing the failure of one system from compromising the security of the information is referred to as **redundancy**.
- Redundancy can be implemented at a number of points throughout the security architecture, such as firewalls, proxy servers, and access controls.
- The use of firewalls and intrusion detection systems(IDS) that use both packet-level rules and data content analysis.




### Security Perimeter

- A Security Perimeter is the first level of security that protects all internal systems from outside threats.
- Unfortunately, the perimeter does not protect against internal attacks from employee threats, or on-site physical threats.
- Security perimeters can effectively be implemented as multiple technologies that segregate the protected information from those who would attack it.

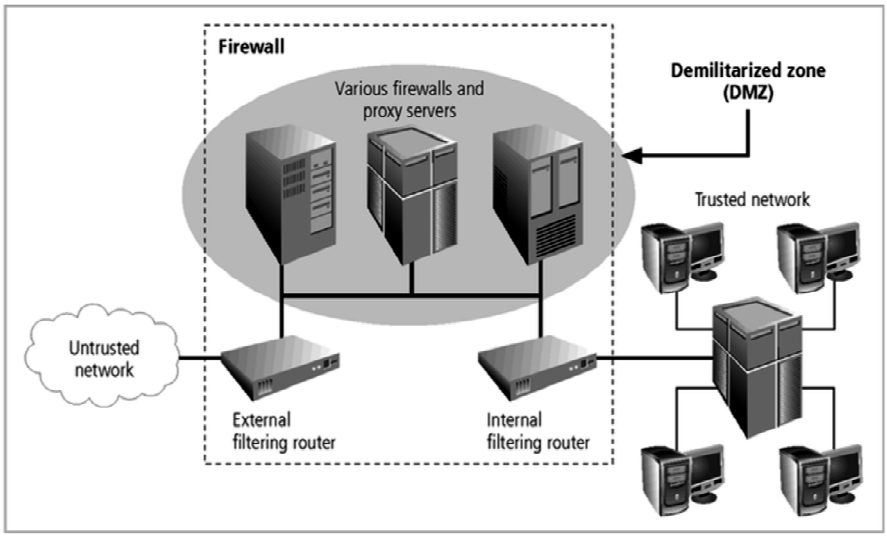
- Within security perimeters the organization can establish security domains, or areas of trust within which users can freely communicate.
- The presence and nature of the security perimeter is an essential element of the overall security framework, and the details of implementing the perimeter make up a great deal of the particulars of the completed security blueprint.
- The key components used for planning the perimeter are presented in the following sections on firewalls, DMZs, proxy servers, and intrusion detection systems.



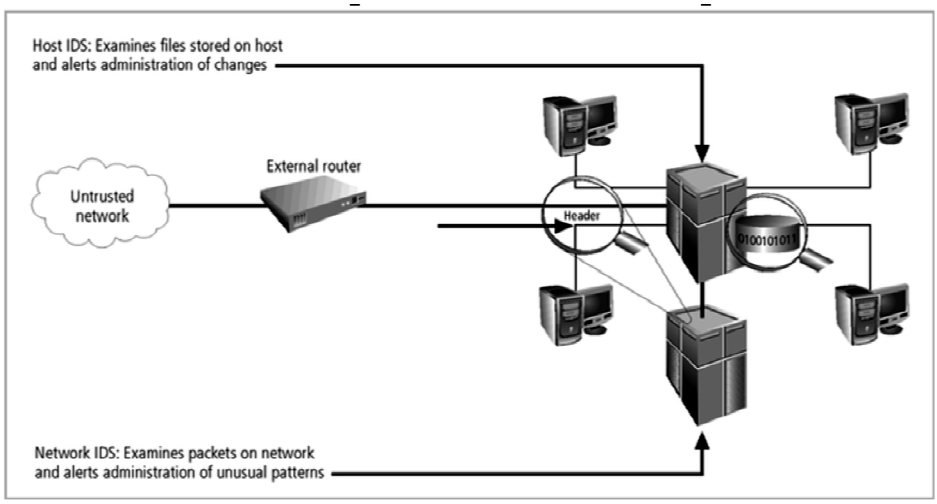

**Key Technology Components**

Other key technology components

- A **firewall** is a device that selectively discriminates against information flowing into or out of the organization.
- Firewalls are usually placed on the security perimeter, just behind or as part of a **gateway router**.
- Firewalls can be packet filtering, stateful packet filtering, proxy, or application level.
- A Firewall can be a single device or a **firewall subnet**, which consists of multiple firewalls creating a buffer between the outside and inside networks.
- The **DMZ** (demilitarized zone) is a no-man's land, between the inside and outside networks, where some organizations place Web servers
- These servers provide access to organizational web pages, without allowing Web requests to enter the interior networks.
- **Proxy server-** An alternative approach to the strategies of using a firewall subnet or a DMZ is to use a **proxy server**, or **proxy firewall**.
- When an outside client requests a particular Web page, the proxy server receives the request as if it were the subject of the request, then asks for the same information from the true Web server(acting as a proxy for the requestor), and then responds to the request as a proxy for the true Web server.
- For more frequently accessed Web pages, proxy servers can cache or temporarily store the page, and thus are sometimes called **cache servers.**




- **Intrusion Detection Systems (IDSs).** In an effort to detect unauthorized activity within the inner network, or on individual machines, an organization may wish to implement **Intrusion Detection Systems or IDS**.
- **IDs** come in two versions. Host-based & Network-based IDSs.
- **Host-based IDSs** are usually installed on the machines they protect to monitor the status of various files stored on those machines.
- **Network-based IDSs** look at patterns of network traffic and attempt to detect unusual activity based on previous baselines.
- This could include packets coming into the organization's networks with addresses from machines already within the organization (IP spoofing).
- It could also include high volumes of traffic going to outside addresses (as in cases of data theft) or coming into the network (as in a denial of service attack).
- Both host-and network based IDSs require a database of previous activity.



## 3.5 Security Education/Training and Awareness Program

**Q7. What are 3 types of security awareness program?**

*Ans :*

- As soon as general security policy exists, policies to implement **security education, training and awareness (SETA)** program should follow.
- SETA is a control measure designed to reduce accidental security breaches by employees.
- Security education and training builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely
- The SETA program consists of three elements: security education; security training; and security awareness
- The purpose of SETA is to enhance security by:
  - Improving awareness of the need to protect system resources.
  - Developing skills and knowledge so computer users can perform their jobs more securely.
  - Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

| | Education | Training | Awareness |
|---|---|---|---|
| **Attribute** | Why | How | What |
| **Level** | Insight | Knowledge | Information |
| **Objective** | Understanding | Skill | Exposure |
| **Teaching** | Theoretical instruction | Practical instruction | Media |
| **method** | • Discussion seminar | • Lecture | • Videos |
| | • Background reading | • Case study workshop | • Newsletters |
| | • Hands-on practice | • Posters | |
| **Test measure** | Essay (interpret learning) | Problem solving (apply learning) | • True or false<br>• Multiple choice (identify learning) |
| **Impact timeframe** | Long term | Intermediate | Short term |

### Security Education

- Everyone in an organization needs to be trained and aware of information security, but not every member of the organization needs a formal degree or certificate in information security.
- A number of universities have formal coursework in information security.
- For those interested in researching formal information security programs, there are resources available, such as the NSA-identified Centers of Excellence in Information Assurance Education.

### Security Training

- It involves providing members of the organization with detailed information and hands-on instruction to prepare them to perform their duties securely.

- Management of information security can develop customized in-house training or outsource the training program.

**Security Awareness**

- One of the least frequently implemented, but most beneficial programs is the security awareness program
- Designed to keep information security at the forefront of users' minds
- Need not be complicated or expensive
- If the program is not actively implemented, employees may begin to "tune out" and risk of employee accidents and failures increases

**Contingency Planning (CP)**

- Contingency Planning (CP) comprises a set of plans designed to ensure the effective reaction and recovery from an attack and the subsequent restoration to normal modes of business operations.
- Organizations need to develop disaster recovery plans, incident response plans, and business continuity plans as subsets of an overall CP.
- An **incident response plan (IRP)** deals with the identification, classification, response, and recovery from an incident, but if the attack is disastrous(e.g., fire, flood, earthquake) the process moves on to disaster recovery and BCP
- A **disaster recovery plan (DRP)** deals with the preparation for and recovery from a disaster, whether natural or man-made and it is closely associated with BCP.
- A **Business continuity plan (BCP)** ensures that critical business functions continue, if a catastrophic incident or disaster occurs. BCP occurs concurrently with DRP when the damage is major or long term, requiring more than simple restoration of information and information resources.

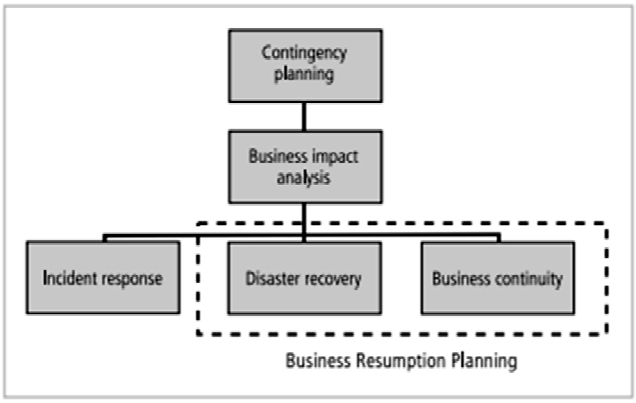
## 3.6 CONTINGENCY PLANNING

**Q8. Explain the key technological components used in security implementation?**

*Ans :*

There are six steps to contingency planning. They are

1. Identifying the mission-or business-critical functions,
2. Identifying the resources that support the critical functions,
3. Anticipating potential contingencies or disasters,
4. Selecting contingency planning strategies,
5. Implementing the contingencies strategies,
6. and Testing and revising the strategy.




**Incident response plan (IRP)**

- It is the set of activities taken to plan for, detect, and correct the impact of an incident on information assets.
- IRP consists of the following 4 phases:
  1. Incident Planning
  2. Incident Detection
  3. Incident Reaction
  4. Incident Recovery

**Incident Planning**

- Planning for an incident is the first step in the overall process of incident response planning.
- The planners should develop a set of documents that guide the actions of each involved individual who reacts to and recovers from the incident.
- These plans must be properly organized and stored to be available when and where needed, and in a useful format.

**Incident Detection**

- Incident Detection relies on either a human or automated system, which is often the help desk staff, to identify an unusual occurrence and to classify it properly as an incident.
- The mechanisms that could potentially detect an incident include intrusion detection systems (both host-based and network based), virus detection software, systems administrators, and even end users.
- Once an attack is properly identified, the organization can effectively execute the corresponding procedures from the IR plan. Thus, **incident classification** is the process of examining a potential incident, or **incident candidate**, and determining whether or not the candidate constitutes an actual incident.
- **Incident Indicators**- There is a number of occurrences that could signal the presence of an incident candidate.
- **Donald Pipkin**, an IT security expert, identifies three categories of incident indicators: **Possible, Probable, and Definite Indicators**.

**Possible Indicators**- There are 4 types of possible indicators of events ,they are,

1. Presence of unfamiliar files.
2. Presence or execution of unknown programs or processes.
3. Unusual consumption of computing resources
4. Unusual system crashes

**Probable Indicators**- The four types of probable indicators of incidents are

1. Activities at unexpected times.
2. Presence of new accounts
3. Reported attacks
4. Notification from IDS

**Definite Indicators-** The five types of definite indicators of incidents are

1. Use of Dormant accounts
2. Changes to logs
3. Presence of hacker tools
4. Notifications by partner or peer
5. Notification by hacker

**Incident Reaction**

- It consists of actions outlined in the IRP that guide the organization in attempting to stop the incident, mitigate the impact of the incident, and provide information for recovery from the incident.
- These actions take place as soon as the incident itself is over.
- In reacting to the incident there are a number of actions that must occur quickly, including notification of key personnel and documentation of the incident.
- These must have been prioritized and documented in the IRP for quick use in the heat of the moment.

**Incident Recovery**

- The recovery process involves much more than the simple restoration of stolen, damaged, or destroyed data files. It involves the following steps.
  - Identify the Vulnerabilities
  - Address the safeguards.
  - Evaluate monitoring capabilities
  - Restore the data from backups.
  - Restore the services and processes in use.
  - Continuously monitor the system
  - Restore the confidence of the members of the organization's communities of interest.

**Disaster Recovery Plan (DRP)**

- DRP provides detailed guidance in the event of a disaster and also provides details on the roles and responsibilities of the various individuals involved in the disaster recovery effort, and identifies the personnel and agencies that must be notified.
- At a minimum, the DRP must be reviewed during a walk-through or talk-through on a periodic basis.

**Many of the same precepts of incident response apply to disaster recovery:**

1. There must be a clear establishment of priorities
2. There must be a clear delegation of roles and responsibilities
3. Someone must initiate the alert roster and notify key personnel.
4. Someone must be tasked with the documentation of the disaster.
5. If and only if it is possible, attempts must be made to mitigate the impact of the disaster on the operations of the organization.

**Business Continuity Plan (BCP)**

- It prepares an organization to reestablish critical business operations during a disaster that affects operations at the primary site.
- If a disaster has rendered the current location unusable for continued operations, there must be a plan to allow the business to continue to function.

**Developing Continuity Programs**

- Once the incident response plans and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support the continued viability of the business in the event of a disaster.
- The development of the BCP is simpler than that of the IRP and DRP ,in that it consists of selecting a continuity strategy and integrating the off-site data storage and recovery functions into this strategy.

**Continuity Strategies**

- There are a number of strategies from which an organization can choose when planning for business continuity.
- The determining factor in selection between these options is usually cost.
- In general there are three exclusive options: Hot sites, Warm Sites, and Cold sites; and three shared functions: Time-share, Service bureaus, and Mutual Agreements.

  **Hot sites**: A hot site is a fully configured facility, with all services, communications links, and physical plant operations including heating and air conditioning. It is the pinnacle of contingency planning, a duplicate facility that needs only the latest data backups and the personnel to function as a fully operational twin of the original. Disadvantages include the need to provide maintenance for all the systems and equipment in the hot site, as well as physical and information security.

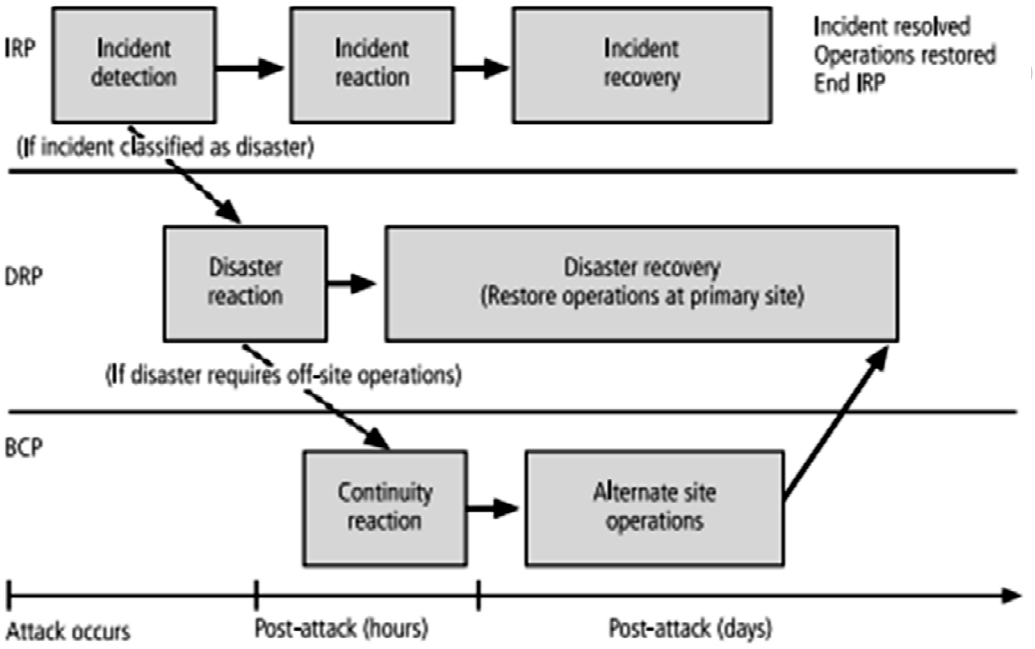
  **Warm sites**: A warm site includes computing equipment and peripherals with servers but not client work stations. It has many of the advantages of a hot site, but at a lower cost.

  **Cold Sites**: A cold site provides only rudimentary services and facilities, No computer hardware or peripherals are provided. Basically a cold site is an empty room with heating, air conditioning, and electricity. The main advantage of cold site is in the area of cost.

**Time-shares**: It allows the organization to maintain a disaster recovery and business continuity option, but at a reduced overall cost. The advantages are identical to the type of site selected(hot, warm, or cold). The disadvantages are the possibility that more than one organization involved in the time share may need the facility simultaneously and the need to stock the facility with the equipment and data from all organizations involved, the negotiations for arranging the time-share, and associated arrangements, should one or more parties decide to cancel the agreement or to sublease its options.

**Service bureaus:** A service bureau is an agency that provides a service for a fee. In the case of disaster recovery and continuity planning, the service is the agreement to provide physical facilities in the event of a disaster. These types of agencies also provide off-site data storage for a fee. The disadvantage is that it is a service, and must be renegotiated periodically. Also, using a service bureau can be quite expensive.

**Mutual Agreements:** A mutual agreement is a contract between two or more organizations that specifies how each will assist the other in the event of a disaster.




## 3.7 FIREWALLS AND VPNS LEARNING OBJECTIVES

**Q9. Explain in detail different firewall architectures?**

*Ans :*

**I.** Understand the role of physical design in the implementation of a comprehensive securityprogram.

**II.** Understand firewall technology and the various approaches to firewall implementation.

**III.** Identify the various approaches to remote and dial-up access protection-that is, how these connection methods can be controlled to assure confidentiality of information, and the authentication and authorization of users.

**IV.** Understand content filtering technology.

**V.** Describe the technology that enables the use of Virtual Private Networks.

As one of the methods of control that go into a well-planned information security program, technical controls are essential in enforcing policy for many IT functions that do not involve direct human control. Networks and computer systems make millions of decisions every second and operate in ways and at speeds that people cannot control in real time. Technical control solutions, properly implemented, can improve an organization's ability to balance the often conflicting objectives of making information more readily and widely available against increasing the information's levels of confidentiality and integrity.

**Physical Design**

- The physical design of an information security program is made up of two parts: Security Technologies and physical security.
- Physical design extends the logical design of the information security program- which is found in the information security blueprint and the contingency planning elements-and makes it ready forimplementation.
- Physical design encompasses the selection and implementation of technologies and processes that mitigate risk from threats to the information assets of organization assets of an organization.

**The physical design process**

1. Selects specific technologies to support the information security blueprint identifies complete technical solutions based on these technologies, including deployment, operations, and maintenance elements, to improve the security of theenvironment.
2. Designs physical security measures to support the technicalsolution.
3. Prepares project plans for the implementation phase thatfollows.

**Firewalls**

- A firewall in an information security program is similar to a building's firewall in that it prevents specific types of information from moving between the outside world, known as the untrusted network(eg., the Internet), and the inside world, known as the trustednetwork.
- The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices.

**Firewall Categorization Methods:**

- Firewalls can be categorized by processing mode, development era, orstructure.
- There are FIVE major processing –mode categories of firewalls: Packet filtering Firewalls, Application gateways, Circuit gateways, MAC layer firewalls and Hybrids.(Hybrid firewalls use a combination of other three methods, and in practice, most firewalls fall into thiscategory)
- Firewalls categorized by which level of technology they employ are identified by generation, with the later generations being more complex and more recently developed.
- Firewalls categorized by intended structure are typically divided into categories including residentialor commercial-grade,hardware-based, software-based, or appliance-baseddevices.

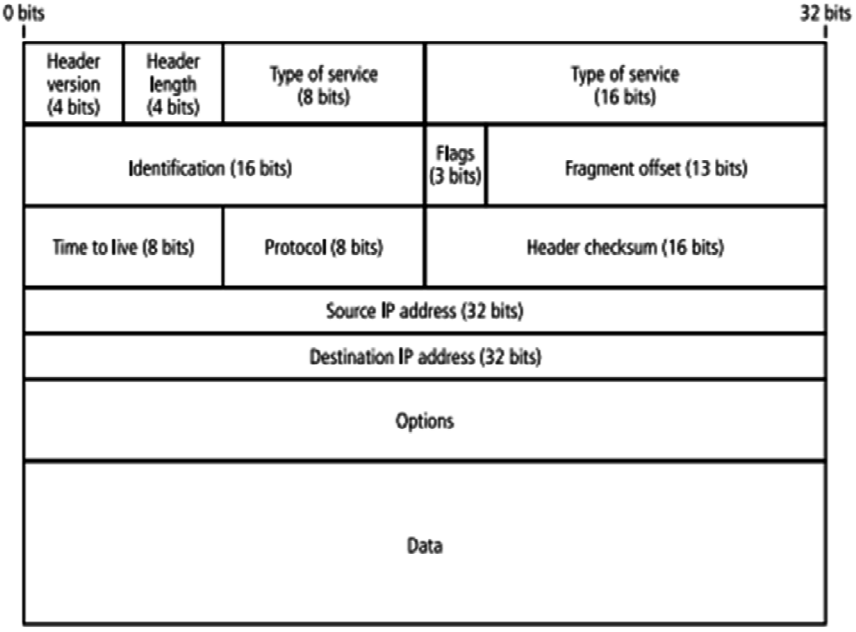
**Firewalls categorized by processing mode:**

The FIVE processing modes are:

1. Packet Filtering
2. Application Gateways
3. CircuitGateways
4. MAC layerfirewalls
5. Hybrids

### Packet Filtering

Packet filtering firewall or simply filtering firewall examine the header information of data packets that come into a network. A packet filtering firewall installed on a TCP/IP based network typically functions at the Ip level and determines whether to drop a packet (Deny) or forward it to the next network connection (Allow) based on the rules programmed into the firewall. Packet filtering firewalls examine evry incoming packet header and can selectively filter packets based on header information such as destination address, source address, packet types, and other key information.

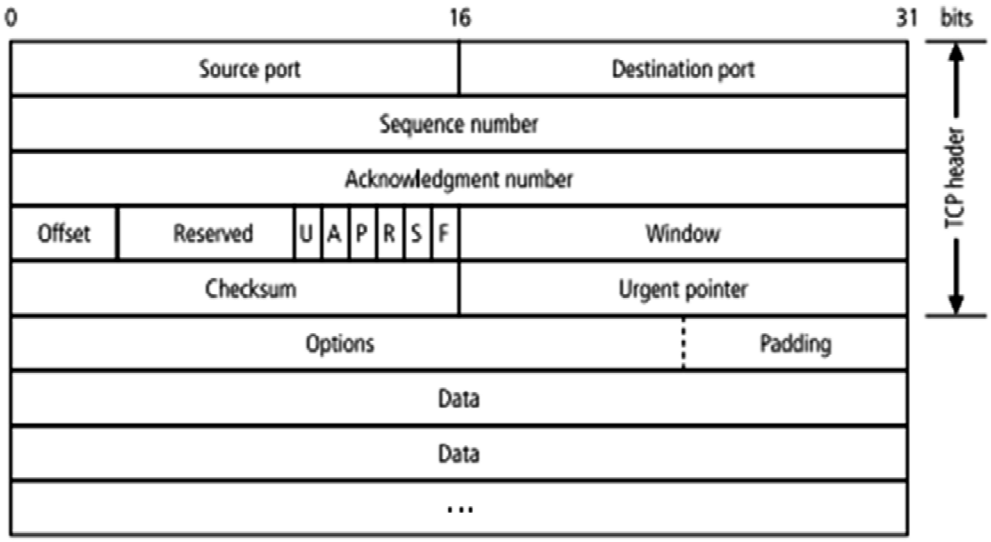


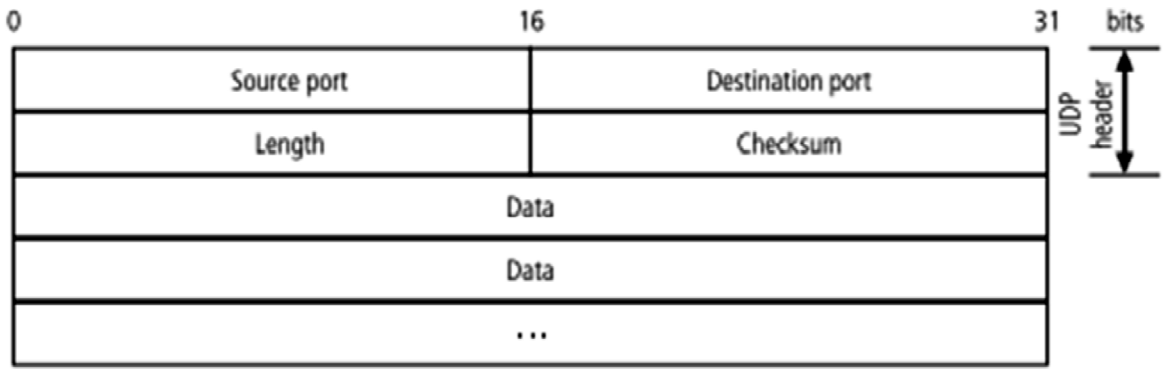

Packet Filtering firewalls san network data packets looking for compliance with or vilation of the rules of the firewalls database.Filtering firewalls inspect packets at the network layer, or Layer 3 of the OSI model. If the device finds a packet that matches a restriction, it stops the packet from travelling from one network to another.

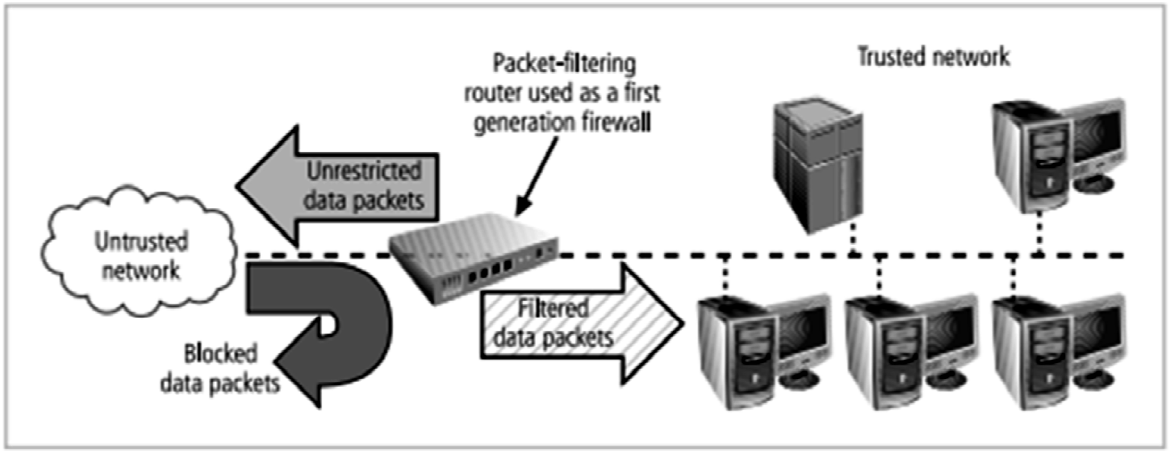
The restrictions most commonly implemented in packet filtering firewalls are based on a combination of the following:

1. IP source and destinationaddress.
2. Direction (in bound oroutbound)
3. Transmission Control Protocol (TCP) or User Datagram protocol(UDP) source and destination portrequests.

A packets content will vary in structure, depending on the nature of the packet. The two primary service types are TCP and UDP. The structure of these two major elements of the combined protocol known as TCP/IP Simple firewall models examine TWO aspects of the packet header: the destination and source address. They enforce address restrictions, rules designed to prohibit packets with certain address or partial addresses from passing through the device.They accomplish this through access control lists(ACLs), which are created and modified by the firewall administrators. How a packet filtering router can be used as a simple firewall to filter data packets from inbound connections and allow outbound connections unrestricted access the public network.




For an example of an address restriction scheme. If an administrator were to configure a simple rule based on the content of the table, any attempt to connect that was made by an external computer or network device in the 192.168.*.* address range (192.168.0.0- 192.168.255.255) would be aloowed. The ability to restrict a specific service , rather than just a range of IP address, is available in a more advanced version of this first generation firewall.

| Source Address | Destination Address | Service (HTTP, SMTP, FTP, Telnet) | Action (Allow or Deny) |
|---|---|---|---|
| 172.16.x.x | 10.10.x.x | Any | Deny |
| 192.168.x.x | 10.10.10.25 | HTTP | Allow |
| 192.168.0.1 | 10.10.10.10 | FTP | Allow |

The ability to restrict a specific service is now considered standard in most routers and is invisible to the user. Unfortunately, such systems are unable to detect the modification of packet headers, which occurs in some advanced attack methods, including IP spoofing attacks.

There are THREE subsets of packet filtering firewalls: Static filtering, Dynamic Filtering, and stateful inspection

- **Static Filtering:** Static filtering requires that the filtering rules governing how the firewall decides which packets are allowed and which are denied are developed and installed. This type of filtering is common in network routers andgateways.
- **Dynamic Filtering: Dynamic Filtering allows to react to an emergent event and update or create** rules to deal with the event. This reaction could be positive , as in allowing an internal user to engage in a specific activity upon request, or negative as in dropping all packets from a particular address when an increase in the presence of a particular type of malformed packet is detected.

  While static filtering firewalls allow entire sets of one type of packet to enter in response to authorized requests, the dynamic packet filtering firewall allows only a particular packet with a particular source, destination, and port address to enter through the firewall. It does this by opening and closing doors in the firewall based on the information contained in the packet header, which makes dynamic packet filters an intermediate form, between traditional static packet filters and application proxies.
- **Stateful Inspection:** Stateful Inspection firewalls , also called stateful firewalls, keep track of each network connection between internal and external systems using a state table.

  A state table tracks the state and context of each packet in the conversation by recording which station sent what packet and when.Staeful inspection firewalls perform packet filtering like they can block incoming packets that are not responses to internal requests. If the state fulfire wall receives an incoming packet that it cannot match in its state table, it defaults to its ACL to determine whether to allow the packet to pass.

The primary disadvantage of this type of firewall is the additional processing required to manage and verify packets against the state table, which can leave the system vulnerable to a Dos or DDoS attack.In such an attack, the firewall system receives a large number of external packets, which slows the firewall because it attempts to compare all of the incoming packets first to the state table and then to the ACL.

On the positive side, these firewalls can track connectionless packet traffic, such as UDP and remote procedure calls (RPC) traffic.

Dynamic stateful filtering firewalls keep a dynamic state table to make changes within predefined limits tot eh filtering rules based on events as they happen.A state table looks similar to a firewall rule set but has additional information.

The state table contains the familiar source IP and port , and destination IP and port , but ads information on the protocol used (UDP or TCP), total time in seconds, and time remaining in seconds.Many state table implementations allow a connection to remain in place for up to 60 minutes without any activity before the state is deleted.

The example shown in Table shows this in column labeled Total Time. The time remaining column shows a countdown of the time that is left until the entry is deleted.

| Source Address | Source Port | Destination Address | Destination Port | Time Remaining in Seconds | Total Time in Seconds | Protocol |
|---|---|---|---|---|---|---|
| 192.168.2.5 | 1028 | 10.10.10.7 | 80 | 2725 | 3600 | TCP |

**ApplicationGateways**

The application gateway, also known as an application –level firewall or application firewall, is frequently installed on a dedicated computer, separate from the filtering router, but is commonly used in conjunction with a filtering router. The application firewall is also known as a proxy server, since it runs special software that acts as a proxy for a service request.

An organization that runs a Web server can avoid exposing thee server to direct traffic from users by installing a proxy server, configured with the registered domain's URL. This proxy server will then receive requests for Web pages, access the Web server on behalf of the external client, and return the requested pages to the users.these servers can store the most recently accessed pages in their requested pages to the users. These servers can store the most recently accessed pages in their internal cache, and are thus also called cache servers.The benefits from this type of implementation are significant.

One common example of an application –level firewall or proxy server is a firewall that blocks all requests for an responses to requests from Web pages and services from the internal computers of an organization, and instead makes all such requests and responses go to intermediate computers or proxies in the less protected areas of the organizations network.This techniques of using proxy servers is still widely used to implement electronic commerce functions.

The primary dis-advantage of application-level firewalls is that they are designed for specific protocol and cannot easily be reconfigured to protect against attacks on other protocols. Since application firewalls work at the application layer they are typically restricted to a single application (Eg, FTP, Telnet, HTTP, SMTP, SNMP). The processing time and resources necessary to read each packet down to the application layer diminishes the ability of these firewalls to handle multiple types of applications.

**CircuitGateways**

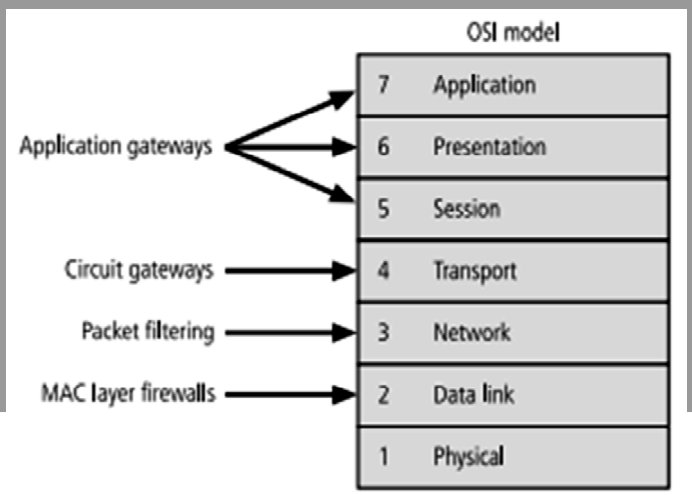
The circuit firewall operates at the transport layer. Again connections are authorized based on addresses. Like filtering firewalls, circuit gateways firewalls do not usually look at data traffic flowing between

one network and another, but they do prevent direct connections between one network and another. They accomplish this by creating tunnels connecting specific processes or systems on each side of the firewall,and then allow only authorized traffic, such as a specific type of TCP connection for only authorized users, in these tunnels.

Writing for NIST in SP 800-110, John Wack describes the operation of a circuit gateway as follows: " A circuit-level gateway relays TCP connections but does no extra processing or filtering of the protocol. For example, the use of a TELNET application server is a circuit –level gateway operation, since once the connection between the source and destination is established, the firewall simply passes bytes between the systems without further evaluation of the packet contents. Another example of a circuit –level gateway would be for NNTP, in which the NNTP server would connect to the firewall, and then internal systems NNTP clients would connect to the firewall. The firewall would again, simply pass bytes.

### MAC layerFirewalls

MAC layer firewalls are designed to operate at the media access control layer of the OSI network mode. This gives these firewalls the ability to consider the specific host computer's identity in its filtering decisions. Using this approach, the MAC addresses the specific host computers are linked to ACL entries that identify the specific types of packets that can be sent to each host, and all other traffic is blocked.




### HybridFirewalls

Hybrid Firewalls combine the elements of other types of firewalls-that is, the elements of packet filtering and proxy services, or of packet filtering and circuit gateways. Alternately, a hybrid firewall system may actually consist of two separate firewall devices: each is a separate firewall system, but they are connected so that they work in tandem. For example, a hybrid firewall system might include a packet filtering firewall that is set up to screen all acceptable requests then pass the requests to a proxy server, which in turn, requests services from a Web server deep inside the organization's networks. An added advantage to the hybrid firewall approach is that it enables an organization to make a security improvement without completely replacing its existing firewalls.

## 3.8 Firewalls Categorized by Development Generation

**Q10. Explain in detail firewalls categorized by processing model different generation of firewalls?**

*Ans :*

The first generation of firewall devices consists of routers that perform only simple packet filtering operations. More recent generations of firewalls offer increasingly complex capabilities, including the increased security and convenience of creating a DMZ-demilitarized zone. At present time, there are five generally recognized generations of firewalls, and these generations can be implemented in a wide variety ofarchitectures.

- **First Generation**: First generation firewalls are static packet filtering firewalls- that is, simple networking devices that filter packets according to their headers as the packets travel to and from the organization'snetworks.
- **Second generation**: Second generation firewalls are application-level firewalls or proxy servers- that is, dedicated systems that are separate from the filtering router and that provide intermediate services forrequestors.
- **Third Generation**: Third generation firewalls are stateful inspection firewalls, which as you may recall, monitor network connections between internal and external systems using statetables.
- **Fourth Generation**: While static filtering firewalls, such as first and third generation firewalls, allow entire sets of one type of packet to enter in response to authorized requests, the fourth generation firewalls, which are also known as dynamic packet filtering firewalls, allow only a particular packet with a particular source , destination, and port address toenter.
- **Fifth Generation**:The fifth generation firewall is the kernel proxy, a specialized form that works under the Windows NT Executive, which is the kernel of Windows NT. This type of firewall evaluates packets at multiple layers of the protocol stack, by checking security in the kernel as data is passed up and down the stack. Cisco implements this technology in the security kernel of its Centri firewall. The Cisco security kernel contains three component technologies: The Interceptor/Packet analyser, the securittanalyser, the security verification engine (SVEN), and kernel Proxies. The interceptor captures packets arriving atthe firewall server and passes them to the packet analyzer., which reads the header information, extracts signature data,and passes both the data and the packet, map it to an exisiting session, or create a new session. If a current session exists, the SVEN passes the information through a custom-built protocol stack created specifically for that session. The temporary protocol stack uses a customized implementation of the approach widely known as Network Address Translation (NAT). The SVEN enforces the security policy that is configured into the Kernel Proxy as it inspects eachpacket.

### Firewalls Categorized by Structure

Firewalls can also be categorized by the structure used to implement them; Most commercial grade firewalls are dedicated appliances. That is , they are stand –alone units running on fully customized computing platforms that provide both the physical network connection and firmware programming necessary to perform their function, whatever that function (static filtering, application proxy etc.,) may be. Some

firewall applications use highly customized, sometimes proprietary hardware systems that are developed exclusively as firewall devices. Other commercial firewall systems are actually off-the- shelf general purpose computer systems. These computers then use custom application software running either over standard operating systems like Windows or Linux/Unix or on specialized variants of these operating systems. Most small office or residential-grade firewalls are either simplified dedicated appliances running on computing devices, or application software installed directly on the user's computer.

### Commercial –Grade Firewall Appliances

Firewall appliances are stand-alone, self-contained combinations of computing hardware and software. These devices frequently have many of the features of a general purpose computer with the addition of firmware based instructions that increase their reliability and performance and minimize the likelihood of being compromised. The customized software operating system that drives the device can be periodically upgraded, but can only be modified using a direct physical connection or after using extensive authentication and authorization protocols. The firewall rule sets are stored in non- volatile memory, and thus they can be changed by technical staff when necessary but are available each time the device isrestarted.

Commercial Grade Firewall Systems: A commercial-grade firewall system consists of application software that is configured for the requirements of the firewall application and running on a general purpose computer. Organizations can install firewall software on an existing general purpose computer system, or they can purchase hardware that has been configured to the specifications that yield optimum performance for the firewall software. These systems exploit the fact that firewalls are essentially application software packages that use common general-purpose network connections to move data from one network to another.

Small Office/Home Office (SOHO) Firewall Applications: S more and more small business and residences obtain fast Internet connections with digital subscriber lines (DSL) or cable modem connections, they become more and more vulnerable to attacks. What many small business and work-from-home users don't realize that unlike dial-up connections, these high-speed services are always on and thus the computers connected to them are constantly connected? These computersare,therefore,muchmore likely to show up on the scanning actions performed by hackers than if they were only connected for the duration of a dial-up session. Coupled with the typically lax security capabilities of home computing operating systems like Windows 95, Windows 98 and even Windows Millennium Edition, most of these systems are wide open to outside intrusion. Even Windows XP Home Edition, a home computing operating system which can be securely configured, is often a soft target since few users bother to learn how to configure it securely. Just as organizations must protect their information, residential users must also implement some form of firewall to prevent loss, damage, or disclosure of personal information.

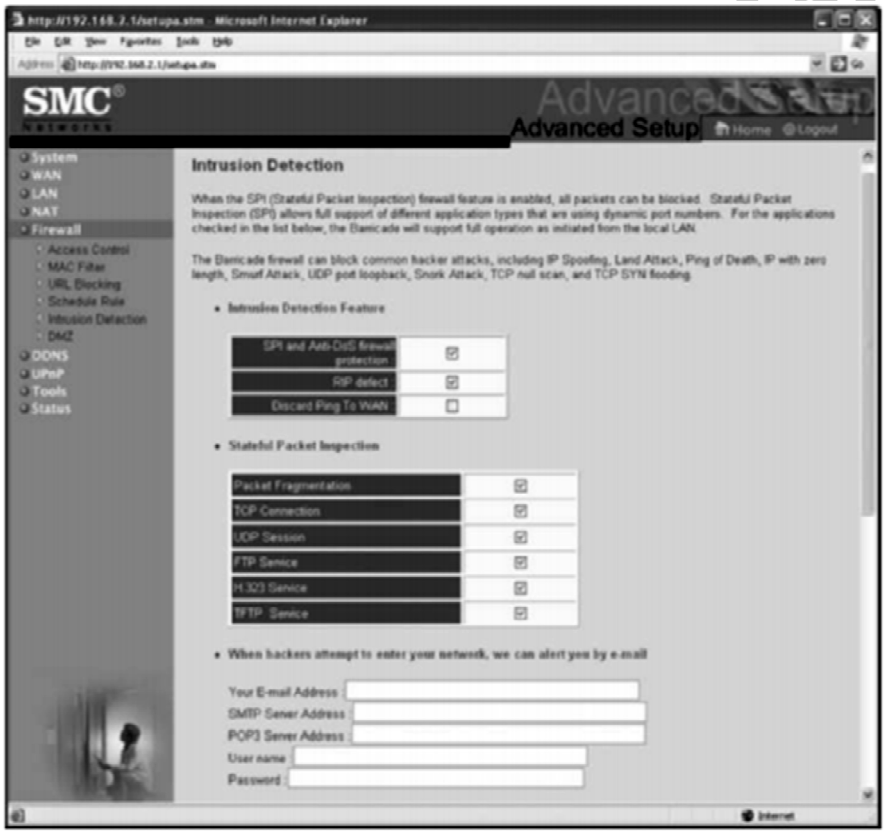
One of the most effective methods of improving computing security in the SOHO setting is through the implementation of a SOHO or residential grade firewall. These devices, also known as broadband gateways or DSL/Cable modem routers , connect the user's local area network or a specific computer system to the Internetworking device-in this case, the cable modem or DSL router provided by the

Internet service provider (ISP). The SOHO firewall servers first as a stateful firewall to enable inside to outside access and can be configured to allow limited TP/IP port forwarding and /or screened subnet capabilities.

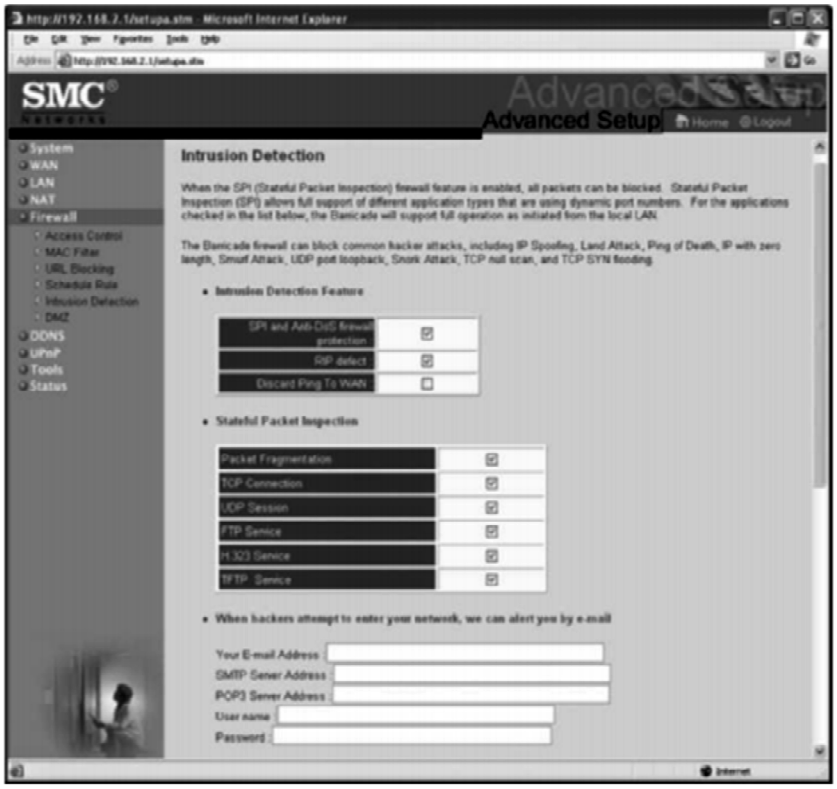
In recent years, the broadband router devices that can function as packet filtering firewalls have been enhanced to combine the features of wireless access points (WAPs) as well as small stackable LAN switches in a single device. These convenient combination devices give the residential/SOHO user the strong protection that comes from the use of Network Address Translation(NAT) services.NAT assigns non-routing local address to the computer systems in the local area network and uses the single ISP assigned address to communicate with the Internet. Since the internal computers are not visible to the public network, they are very much less likely to be scanned or compromised. Many users implement these devices primarily to allow multiple internal users to share a single external Internet connection.

Many of these firewalls provide more than simple NAT services. Some SOHO / residential firewalls include packet filtering, port filtering, and simple intrusion detection systems, and some can even restrict access to specific MAC addresses. Users may be able to configure port forwarding and enable outside users to access specific TCP or UDP ports on specific computers on the protected network.

An example of the set up screen from the SMC Barricade residential broadband router that can be used to identify which computers inside the trusted network may access the Internet.




Some firewall devices are manufactured to provide a limited intrusion detection capability. The configuration screen from the SMC Barricade residential broadband router that enables the intrusion detection feature. When enabled , this feature will detect specific, albeit limited, attempts to compromise the protected network. In addition to recording intrusion attempts, the router can be made to use the contact information provided on this configuration screen to notify the firewall administrator of the occurrence of an intrusion attempt.




A continuation of the configuration screen for the intrusion detection feature. Note that the intrusion criteria are limited in number, but the actual threshold levels of the various activities detected can be customized by the administrator.

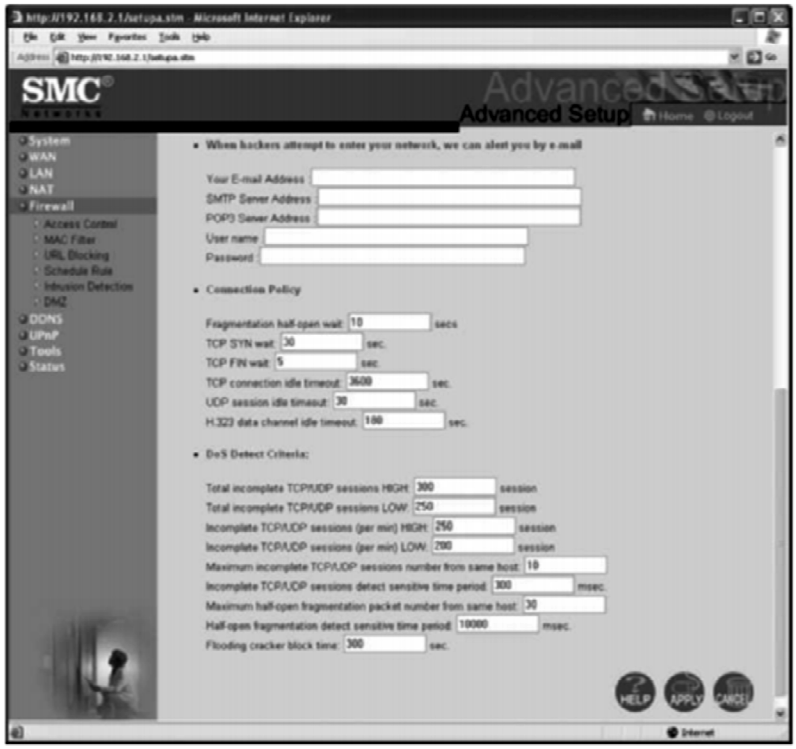
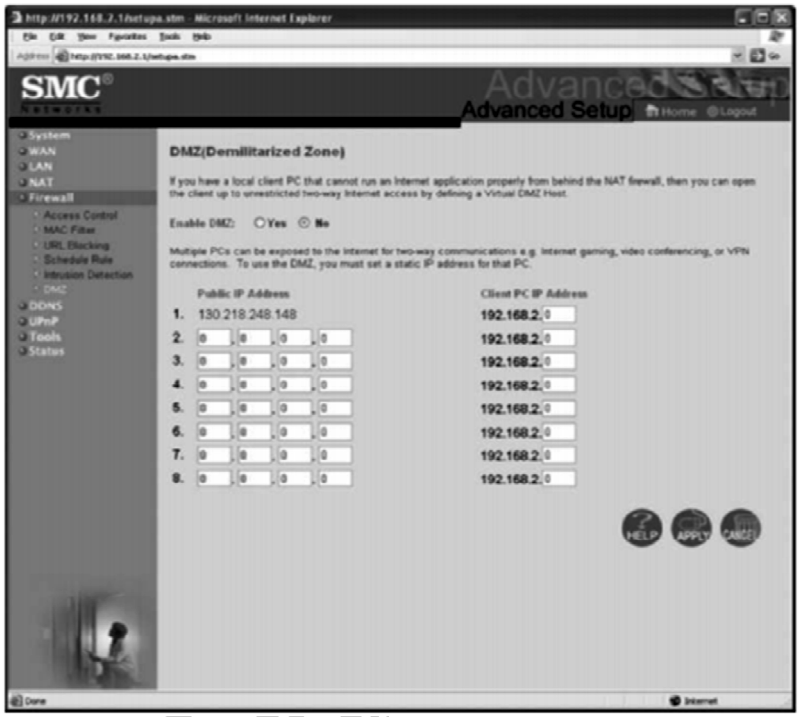


Fig illustrates that even simple residential firewalls can be used to create a logical screened sub network (DMZ) that can provide Web services. This screen shows how barricade can be configured to allow Internet clients' access to servers inside the trusted network. The network administrator is expected to ensure that the exposed servers are sufficiently secured for this type of exposure.




**Residential –Grade Firewall Software:** Another method of protecting the residential user is to install a software firewall directly on the user's system. Many people have elected to implement these residential grade software based firewalls, but , unfortunately , they may not be as fully protected as they think. The majority of individuals who implement a software-based firewall use one of the products listed.

| Firewall (date in parentheses is year posted on *download.cnet.com*) | CNET Editor's Rating (number of stars out of 5) |
|---|---|
| Norton 360 | 4 |
| ZoneAlarm Extreme Security (2010) | 3 |
| Trend Micro Internet Security (2009) | 3.5 |
| Panda Internet Security (2009) | 3.5 |
| McAfee Internet Security (2009) | 3.5 |
| PC Tools Firewall Plus (2009) | 4 |
| Agnitum Outpost Firewall Pro (2009) | 4 |
| Sygate Personal Firewall 5.6.2808 (2007) | 4 |
| AVG Anti-virus plus Firewall 9.0.700 (2009) | unrated |
| Comodo Internet Security 3.12 (2009) | 5 |
| Ashampoo FireWall Free 1.2 (2007) | 5 |
| Webroot AV with AntiSpyware and Firewall 6.1 (2007) | unrated |
| VisNetic Firewall 3.0 (2007) | unrated |
| Kerio WinRoute Firewall 6.7 (2009) | unrated |
| Microsoft Windows Firewall (integral to Windows XP, Vista, 7 systems) | unrated |
| CA Internet Security Suite Plus (2009) | 2.5 |

This list represents a selection of applications that claim to detect and prevent intrusion into the user's system, without affecting usability. The problem is that many of the applications on the list provide free versions of their software that are not fully functional, yet many users implement them thinking their systems are sufficiently protected. But the old adage of you get what you pay for certainly applies to software in this category. Thus, users who implement less-capable software often find that it delivers less complete protection. Some of these applications combine firewall services with other protections like antivirus, or intrusiondetection.

There are limits to the level of configurability and protection that software firewalls can provide. Many of the applications on this list have very limited configuration options ranging from none to low to medium to high security. With only three or four levels of configuration, users may find that the application becomes increasingly difficult to use in everyday situations. They find themselves sacrificing security for usability, as the application, packet, or service to connect internally or externally. The Microsoft windows 2000 and XP versions of Internet explorer have a similar configuration with settings that allow users to choose from a list of preconfigured options, or choose a custom setting with a more detailed security configuration.

Software Vs. hardware: The SOHO firewall debate: So which type of firewall should the residential user implement? There are many users who swear by their software firewalls. Personal experience will produce a variety of opinioned perspectives. Ask yourself this question: where would you rather defend against a hacker? With the software option, the hacker is inside your computer, battling with a piece of software that may not have been correctly installed, configured, patched, upgraded or designed. If the software happens to have known vulnerability, the hacker could bypass it and then have unrestricted access to your system. With the hardware device, even if the hacker manages to crash the firewall system, your computer and information are still safely behind the now disabled connection, which is assigned a non routable IP address making it virtually impossible to reach from the outside.

## 3.9 FIREWALL ARCHITECTURES

**Q11. Write a short notes on (a) Screened subnet fire walls (DMZ) (b) Screened host fire wall.**

*Ans :*

The configuration that works best for a particular organization depends on three factors: The objectives of the network, the organization's ability to develop and implement the architectures, and the budget available for the function.

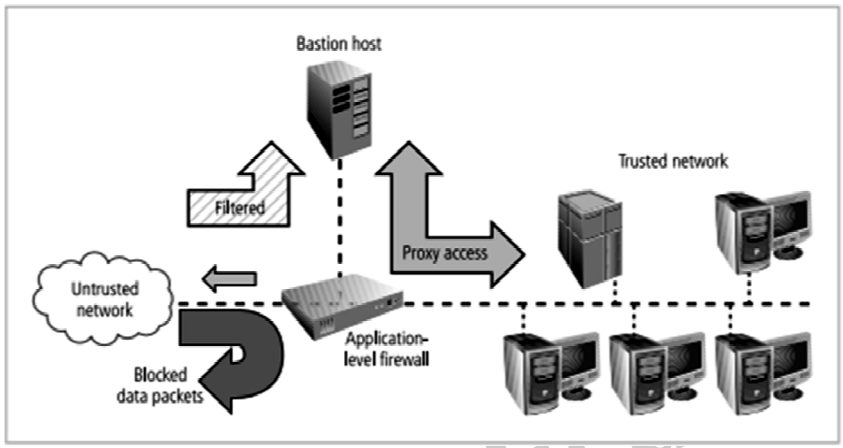
There are FOUR common architectural implementations of firewalls.These implementations are packet filtering routers, screened host firewalls, dual-homed firewalls,and screened subnet firewalls.

Packet Filtering Routers: Most organizations with an Internet connections have some form of a router as the interface to the Internet at the perimeter between the organization's internal networks and the external service provider. Many of these routers can be configured to reject packets that the organization does not allow into the network. This is a simple but effective way to lower the organization's risk from external attack. The drawbacks to this type of system include a lack of auditing and strong authentication. Also, the complexity of the access control lists used to filter the packets can grow and degrade network performance.

Screened Host Fire walls: This architecture combines the packet filtering router with a separate, dedicated firewall, such as an application proxy server. This approach allows the router to pre-screen packets to minimize the network traffic and loads on the internal proxy.The application proxy examines an application layer protocol, such as HTTP, and perform the proxy services. This separate host is often referred to as a bastion host; it can be a rich target for external attacks, and should be very thoroughly

secured. Even though the bastion host/application' proxy actually contains only cached copies of the internal Web documents, it can still present a promising target, because compromise of the bastion host can disclose the configuration of internal networks and possibly provide external sources with internal information. Since the bastion host stands as a sloe defender on the network perimeter, it is also commonly referred to as the Sacrificial Host.

To its advantage, this configuration requires the external attack to compromise two separate systems, before the attack can access internal data. Inthis way, the bastion host protects the data more fully than the router alone. A typical configuration of a screened host architectural approach.



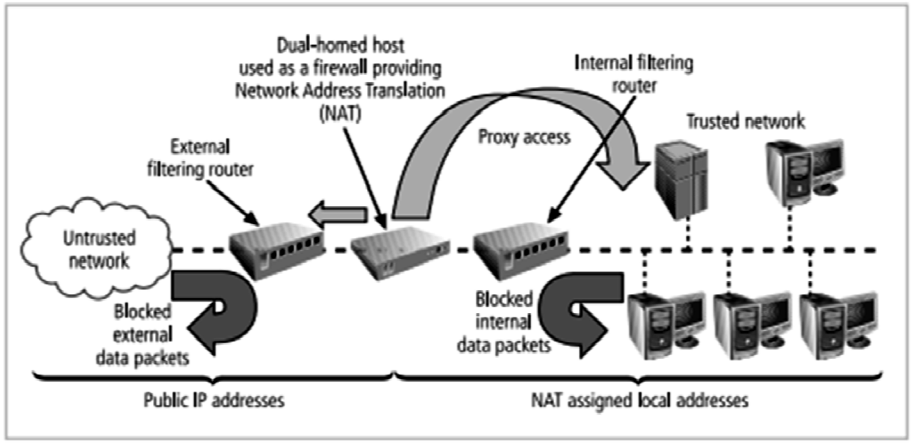

Dual-Homed HostFirewalls: The next step up in firewall architectural complexity is the dual-homed host. When this architectural approach is used, the bastion host contains two NICs (Network Interface Cards) rather than one, as in the bastion host configuration. One NIC is connected to the external network, and one is connected to the internal network, providing an additional layer of protection. With TWO NICs , all traffic must physically go through the firewall to move between the internal and externalnetworks.

Implementation of this architecture often makes use of NATs. NAT is a method of mapping real, valid, external IP addresses to special ranges of non-routable internal IP addresses, thereby creating yet another barrier to intrusion from external attackers.

The internal addresses used by NAT consist of three different ranges. Organizations that need Class A addresses can use the 10.x.x.x range, which has over 16.5 million usable addresses. Organization's that need Class B addresses can use the 192.168.x.x range, which has over 65,500 addresses. Finally ,organiazations with smaller needs , such as those needing onlya few Class C addresses, can use the c172.16.0.0 to 172.16.15.0 range, which hs over 16 Class C addresses or about 4000 usable addresses.

For a recap of the IP address ranges resevedfro non-public networks. Messages sent with internal addresses within these three internal use addresses is directly connected to the external network, and avoids the NAT server, its traffic cannot be routed on the public network. Taking advantage of this , NAT prevents external attacks from reaching internal machines with addresses in specified ranges.If the NAT server is a multi-homed bastion host, it translates between the true, external IP addresses assigned to the organization by public network naming authorities ansd the internally assigned, non- routable IP addresses. NAT translates by dynamically assigning addresses to internal communications and tracking the conversions with sessions to determine which incoming message is a response to which outgoing traffic. Figure shows a typical configuration of a dual homed host firewall that uses NAT and proxy access to protect the internal network.

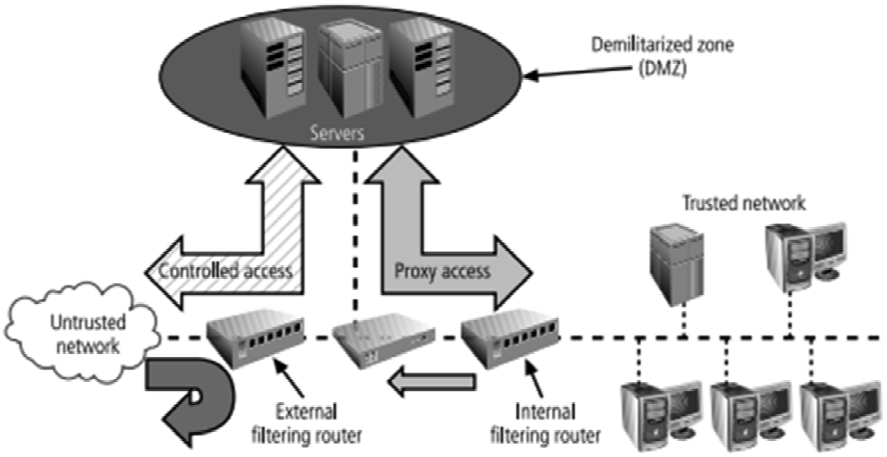
| Class | From | To | CIDR Mask | Decimal Mask |
|---|---|---|---|---|
| Class A or 24 Bit | 10.0.0.0 | 10.255.255.255 | /8 | 255.0.0.0 |
| Class B or 20 Bit | 172.16.0.0 | 172.31.255.255 | /12 or /16 | 255.240.0.0 or 255.255.0.0 |
| Class C or 16 Bit | 192.168.0.0 | 192.168.255.255 | /16 or /24 | 255.255.0.0 or 255.255.255.0 |




Another benefit of a dual-homed host is its ability to translate between many different protocols at their respective data link layers, including Ethernet , Token Ring, Fiber Distributed Data interface (FDDI) , and Asynchronous Transfer Method (ATM). On the downside, if this dual-homed host is compromised, it can disable the connection to the external network, and as traffic volume increases, it can become overloaded. Compared to more complex solutions, however, this architecture provides strong overall protection with minimalexpense.

### Screened Subnet Firewalls (withDMZ)

The dominant architecture used today is the screened subnet firewall. The architecture of a screened subnet firewall provides a DMZ. The DMZ can be a dedicated port on the firewall device linking a single bastion host, or it can be connected to a screened subnet. Until recently , servers providing services through an untrusted network were commonly placed in the DMZ. Examples of these include Web servers, file transfer protocol (FTP) servers, and certain database servers. More recent strategies using proxy servers have provided much more securesolutions.



A common arrangement finds the subnet firewall consisting of two or more internal bastion hosts behind a packet filtering router, with each host protecting the trusted network. There are many variants of the screened subnet architecture. The first general model consists of two filtering routers, with one or more dual-homed bastion hosts between them. In the second general model, the connections are routed asfollows:

i. Connections from the outside or un trusted network are routed through an external filteringrouter.

ii. Connections from the outside or un trusted network are routed into-and then out of – a routing firewall to the separate network segment known as theDMZ.

iii. Connections into the trusted internal network are allowed only from the DMZ bastion hostservers.

The screened subnet is an entire network segment that performs two functions: it protects the DMZs systems and information from outside threats by providing a network of intermediate security; and it protects the internal networks by limiting how external connections can gain access to internal systems. Although extremely secure, the screened subnet can be expensive to implement and complex to configure and manage. The value of the information it protects must justify the cost.

Another facet of the DMZ is the creation of an area of known as an extranet. AN extranet is a segment of the DMZ where additional authentication and authorization controls are put into place to provide services that are not available to the general public. An example would be an online retailer that allows anyone to browse the product catalog and place items into a shopping cart, but will require extra authentication and authorization when the customer is ready to check out and place an order.

## SOCKS SERVER

Deserving of brief special attention is the SOCKS firewall implementation. SOCKS is the protocol for handling TCP traffic through a proxy server. The SOCKS system is a proprietary circuit level proxy server that places special SOCKS client-side agents on each workstation. The general approach is to place the filtering requirements on the individual workstation rather than on a single point of defense (and thus point of failure). This frees the entry router from filtering responsibilities, but it then requires each workstation to be managed as a firewall detection and protection device. A SOCKS system can require support and management resources beyond those usually encountered for traditional firewalls since it is used to configure and manage hundreds of individual clients as opposed to a single device or small set ofdevices.

## Selecting the Right Firewall

When selecting the best firewall for an organization, you should consider a number of factors. The most important of these is the extent to which the firewall design provides the desired protection. When evaluating a firewall , questions should be created that cover the following topics:

- What type of firewall technology offers the right balance between protection and cost for needs of the organization.
- What features are included in the base price? What features are available at extra cost? Are all cost factors known?
- How easy is to set up and configure the firewall?How accessible are the staff technicians who can competently configure the firewall?
- Can the candidate firewall adapt to the growing network in the target organization?
- The second most important issue is the cost. Cost may keep a certain make, model or type out of reach for a particular security solution. As with all security decisions, certain compromises may be necessary in order to provide a viable solution under the budgetary constraints stipulated by management.

## Configuring and managing Firewalls

Once the firewall architecture and technology have been selected, the initial configuration and ongoing management of the firewalls needs to be considered. Good policy and practice dictates that each firewall device whether a filtering router, bastion

host, or other firewall implementation, must have its own set of configuration rules that regulate its actions.

In theory packet filtering firewalls use a rule set made up of simple statements that regulate source and destination addresses identifying the type of requestsand /or the ports to be used and that indicate whether to allow or deny the request.

In actuality, the configuration of firewall policies can be complex and difficult. IT professionals familiar with application programming can appreciate the problems associated with debugging both syntax errors and logic errors. Syntax errors in firewall policies are usually easy to identify, as the systems alert the administrator to incorrectly configured policies. However, logic errors, such as allowing instead of denying, specifying the wrong port or service type, and using the wrong switch, are another story.These and a myriad of other simple mistakes can take a device designed to protect user's communications and turn it into one giant choke point.

A choke point that restricts all communications or an incorrectly configured rule can cause other unexpected results. For example, novice firewall administrators often improperly configure a virus-screening e-mail gateway, which, instead of screening e-mail for malicious code, results in the blocking of all incoming e-mail and causes, understandably, a great deal of frustration among users.

Configuring firewall policies is as much an art as it si a science. Each configuration rule must be carefully crafted, debugged, tested, and placed into the access control list in the proper sequence. The process of writing good, correctly sequenced firewall rules ensures that the actions taken comply with the organization's policy. The process also makes sure that those rules that can be evaluated quickly and govern broad access are performed before those that may take longer to evaluate and affect fewer cases, which in turn, ensures that the analysis is completed as quickly as possible for the largest number of requests. When configuring firewalls, keep one thing in mind: when security rules conflict with the performance of business, security often loses. If users can't work because of a security restriction, the security administration is usually told, in no uncertain terms, to remove the safeguard. In other words, organizations are much more willing tolive withpotential riskthan certainfailure. The following sections describe the best practices most commonly used in firewalls and the best ways to configure the rules that support firewalls.

## 3.10 Best Practices for Firewalls

**Q12. What are the factors to be considered in selecting a right fire wall? Outline some of the best practicies firewall use?**

*Ans :*

1. All traffic from the trusted network is allowed out. This allows members of the organization to access the services they need. Filtering and logging of outbound traffic is possible when indicated by specific organizationalpolicies.
2. The firewall device is never directly accessible from the public network for configuration or management purposes. Almost all administrative access tot eh firewall device is denied to internal users as well. Only authorized firewall administrators access the device through secure authentication mechanisms, with preference for a method that is based on cryptographically strong authentication and uses two-factor access controltechniques.
3. Simple Mail Transport protocol (SMTP) data is allowed to pass through the firewall, but it should all be routed to a well-configured SMTP gateway to filter and route messaging trafficsecurity.
4. All internet Control Message Protocol (ICMP) data should be denied. Known as the Ping service, ICMP is a common method for hacker reconnaissance and should be turned off to preventsnooping.
5. Telnet (Terminal Emulation) access to all internal servers from the public networks should be blocked. At the very least, telnet access to the organization's Domain Name Service (DNS) server should be blocked to prevent illegal zone transfers, and to prevent hackers from taking down the organization's entire network. If internal users need to come

into an organization's network from outside the firewall, the organizations should enable them to use a Virtual Private Network (VPN) client, or other secure system that provides a reasonable level of authentication.

6. When web services are offered outside the firewall, HTTP traffic should be denied from reaching your internal networks through the use of some form of proxy access or DMZ architecture. That way, if any employees are running Web servers for internal use on their desktops, the services are invisible to the outside Internet. If the Web server is behind the firewall, allow HTTP or HTTPS (also known as secure socket layer or SSL) through for the Internet at large to view it. The best solution is to place the Web servers containing critical data inside the network and use proxy services from a DMZ (screened network segment), and also to restrict Web traffic bound for internal network addresses in response to only those requests that originated from internal addresses. This restriction can be accomplished through NAT or other stateful inspection or proxy server firewall approaches. All other incoming HTTP traffic should be blocked. If the Web servers only contain advertising, they should be placed in the DMZ and rebuilt on a timed schedule or when –not if, but when-they are compromised.

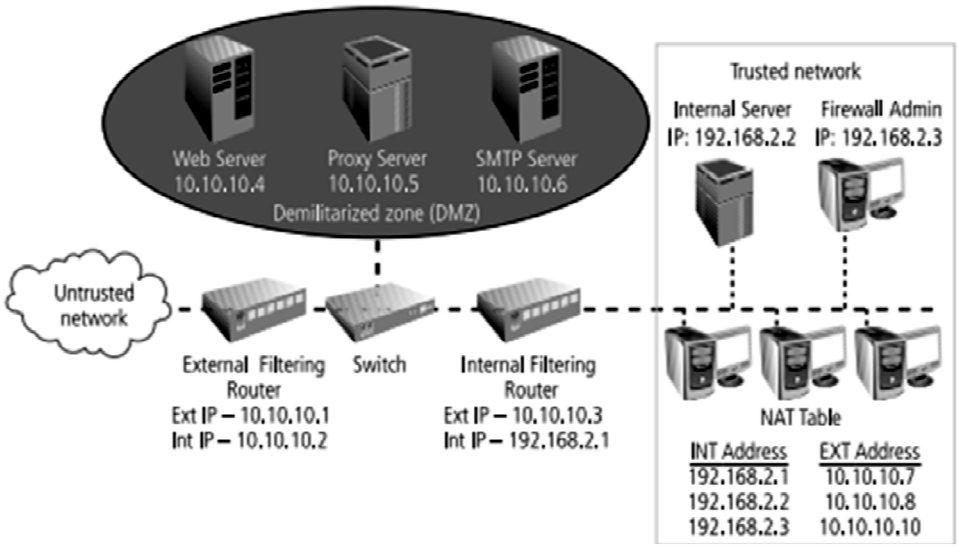
## 3.11 FIREWALL RULES

**Q13. What are wall rule? Explain different firewall rules sets?**

*Ans :*

Firewalls operate by examining a data packet and performing a comparison with some predetermined logical rules. The logic is based on a set of guidelines programmed in by a firewall administrator, or created dynamically and based on outgoing requests for information. This logical set is most commonly referred to as firewall rules, rule base, or firewall logic.

Most firewalls use packet header information to determine whether a specific packet should be allowed to pass through or should be dropped. In order to better understand more complex rules, it is important to be able to create simple rules and understand how they interact.




Some firewalls can filter packets by the name of a particular protocol as opposed to the protocol's usual port numbers. For instance, Telnet protocol packets usually go to TCP port 23, but can sometimes be directed to another much higher port number in an attempt to conceal the activity. The System or

well-known ports are those from 0 through 1023, User or registered ports are those from 1024 through 49151, and Dynamic or Private Ports are those from 49152 through65535.

The following example uses the port numbers associated with several well-known protocols to build a rule base. The port numbers to be used are listed. Note that this is not an exhaustive list.

| Port Number | Protocol |
|---|---|
| 7 | Echo |
| 20 | File Transfer [Default Data] (FTP) |
| 21 | File Transfer [Control] (FTP) |
| 23 | Telnet |
| 25 | Simple Mail Transfer Protocol (SMTP) |
| 53 | Domain Name Services (DNS) |
| 80 | Hypertext Transfer Protocol (HTTP) |
| 110 | Post Office Protocol version 3 (POP3) |
| 161 | Simple Network Management Protocol (SNMP) |

**Rule Set-1:** Responses to internal requests are allowed. In most firewall implementations, it is desirable to allow a response to an internal request for information. In dynamic or stateful firewalls, this is most easily accomplished by matching the incoming traffic to an outgoing request in a state table. In simple packet filtering, this can be accomplished with the following rule for the External Filtering Router. (Note that the network address for the destination ends with .0; some firewalls use a notation of .Xinstead.)

| Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|
| Any | Any | 10.10.10.0 | >1023 | Allow |

From Table, you can see that this rule states that any incoming packet (with any source address and from any source port) that is destined for the internal network (whose destination address is 10.10.10.0) and for a destination port greater than 1023 (that is , any port out of the number range for the well-known ports) is allowed to enter.Why allow all such packets? While outgoing communications request information from a specific port (i.e a port 80 request for a Web page), the response is assigned a number outside the well-known port range. If multiple browser windows are open at the same time, each window can request a packet from a Web site, and the response is directed to a specific destination port, allowing the browser and Web server to keep each conversation separate. While this rule is sufficient for the external router (firewall), it is dangerous simply to allow any traffic in just because it is destined to a high port range. A better solution is to have the internal firewall router use state tables that track connections and prevent dangerous packets from entering this upper port range.

**Rule set-2:** The firewall device is never accessible directly from the public network. If hackers can directly access the firewall, they may be able to modify or delete rules and allow unwanted traffic through. For the same reason, the firewall itself should never be allowed to access other network devices directly. If hackers compromise the firewall and then use its permissions to access other servers or clients, they may cause additional damage or mischief. The rules shown prohibit anyone from directly accessing the firewall and the firewall from directly accessing any other devices. Note that this example is for the external filtering router/firewall only. Similar rules should be crafted for the internal router. Why are there separate rules for each IP addresses? The 10.10.10.1 address regulates external access to and by the firewall, while the 10.10.10.2 address regulates internal access. Not all hackers are outside the firewall!

| Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|
| Any | Any | 10.10.10.1 | Any | Deny |
| Any | Any | 10.10.10.2 | Any | Deny |
| 10.10.10.1 | Any | Any | Any | Deny |
| 10.10.10.2 | Any | Any | Any | Deny |

**Rule set-3:** All traffic from the trusted network is allowed out. As a general rule it is wise not to restrict outgoing traffic, unless a separate router is configured to handle this traffic. Assuming most of the potentially dangerous traffic is inbound, screening outgoing traffic is just more work for the firewalls. This level of trust is fine for most organizations. If the organization wants control over outbound traffic, it should use a separate router.

| Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|
| 10.10.10.0 | Any | Any | Any | Allow |

Why should rule set-3 come after rule set-1 and 2? It makes sense to allow the rules that unambiguously impact the most traffic to be earlier in the list. The more rules a firewall must process to find one that applies to the current packet, the slower the firewall will run. Therefore, most widely applicable rules should come first since the first rule that applies to any given packet will beapplied.

**Rule set-4:** The rule set for the Simple mail Transport Protocol (SMTP) data is shown in Table 6-9. As shown, the packets governed by this rule are allowed to pass through the firewall, but are all routed to a well-configured SMTP gateway. It is important that e-mail traffic reach your e-mail server, and only your e-mail server. Some hackers try to disguise dangerous packets as e-mail traffic to fool a firewall. If such packets can reach only the e- mail server, and the e-mail server has been properly configured, the rest of the network ought to be safe.

| Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|
| Any | Any | 10.10.10.6 | 25 | Allow |

**Rule set-5:** All Internet Control Message Protocol (ICMP) data should be denied. Pings, formally known as ICMP echo requests, are used by internal systems administrators to ensure that clients and servers can reach and communicate. There is virtually no legitimate use for ICMP outside the network, except to test the perimeter routers. ICPM uses port 7 to request a response to a query (eg “Are you there?”) and can be the first indicator of a malicious attack. It’s best to make all directly connected networking devices “black holes” to external probes. Traceroute uses a variation on the ICMP Echo requests, so restricting this one port provides protection against two types of probes. Allowing internal users to use ICMP requires configuring two rules.

| Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|
| 10.10.10.0 | Any | Any | 7 | Allow |
| Any | Any | 10.10.10.0 | 7 | Deny |

The first of these two rules allows internal administrators (and users) to use Ping. Note that this rule is unnecessary if internal permissions rules like those in rule set 2 is used. The second rule in Table does not allow anyone else to use Ping. Remember that rules are processed in order. If an internal user needs to

Ping an internal or external address, the firewall allows the packet and stops processing the rules. If the request does not come from an internal source, then it bypasses the first rule and moves to the second.

**Rule set 6:** Telnet (Terminal emulation) access to all internal servers from the public networks should be blocked. Though not used much in Windows environments, Telnet is still useful to systems administrators on Unix/Linux systems. But the presence of external requests for Telnet services can indicate a potential attack. Allowing internal use of Telnetrequires the same type of initial permission rule you use with P in g.

| Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|
| 10.10.10.0 | Any | 10.10.10.0 | 23 | Allow |
| Any | Any | 10.10.10.0 | 23 | Deny |

**Rule set-7:** when Web services are offered outside the firewall, HTTP traffic should be denied from reaching the internal networks through the use of some form of proxy access or DMZ architecture. With a Web server in the DMZ you simply allow HTTP to access the Web server, and use rule set 8, the Clean Up rule to prevent any other access. In order to keep the Web server inside the internal network, direct all HTTP requests to the proxy server, and configure the internal filtering router/firewall only to allow the proxy server to access the internal Web server.

| Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|
| Any | Any | 10.10.10.4 | 80 | Allow |

This rule accomplishes two things: It allows HTTP traffic to reach the Web server, and it prevents non-HTTP traffic from reaching the Web server. It does the latter through the Clean Up rule (Rule 8). If someone tries to access theWeb server with non-HTTP traffic (other than port 80), then the firewall skips this rule and goes to the next.

The effective use of as proxy server of course requires the DNS entries to be configured as if the proxy server were the Web server. The proxy server would then be configured to repackage any HTTP request packets into a new packet and retransmit to the Web server inside the firewall. Allowing for the retransmission of the repackaged request requires the rule to enable the proxy server at 10.10.10.5 to send to the internal router, presuming the IP address for the internal Web server is 192.168.2.4

The restriction on the source address then prevents anyone else from accessing the Web server from outside the internal filtering router/firewall.

| Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|
| Any | Any | 10.10.10.5 | 80 | Allow |

| Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|
| 10.10.10.5 | any | 10.10.10.8 | 80 | Allow |

**Rule set 8:** The Clean up rule: As a general practice in firewall rule construction, if a request for a service is not explicitly allowed by policy, that request should be denied by a rule. The rule shown in Table 6-15 implements this practice and blocks any requests that aren't explicitly allowed by other rules.

| Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|
| Any | Any | Any | Any | Deny |

Additional rules restricting access to specific servers or devices can be added, but they must be sequenced before the clean up rule. Order is extremely important, as misplacement of a particular rule can result in unforeseen results.

| Rule # | Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|---|
| 1 | 10.10.10.0 | Any | Any | Any | Deny |
| 2 | Any | Any | 10.10.10.1 | Any | Deny |
| 3 | Any | Any | 10.10.10.2 | Any | Deny |
| 4 | 10.10.10.1 | Any | Any | Any | Deny |
| 5 | 10.10.10.2 | Any | Any | Any | Deny |
| 6 | Any | Any | 10.10.10.0 | >1023 | Allow |
| 7 | Any | Any | 10.10.10.6 | 25 | Allow |
| 8 | Any | Any | 10.10.10.0 | 7 | Deny |
| 9 | Any | Any | 10.10.10.0 | 23 | Deny |
| 10 | Any | Any | 10.10.10.4 | 80 | Allow |
| 11 | Any | Any | Any | Any | Deny |

| Rule # | Source Address | Source Port | Destination Address | Destination Port | Action |
|---|---|---|---|---|---|
| 1 | Any | Any | 10.10.10.3 | Any | Deny |
| 2 | Any | Any | 10.10.10.7 | Any | Deny |
| 3 | 10.10.10.3 | Any | Any | Any | Deny |
| 4 | 10.10.10.7 | Any | Any | Any | Deny |
| 5 | Any | Any | 10.10.10.0 | >1023 | Allow |
| 7 | 10.10.10.5 | Any | 10.10.10.8 | Any | Allow |
| 8 | Any | Any | Any | Any | Deny |

Note that the rule allowing responses to internal communications comes first, followed by the four rules prohibiting direct communications to or from the firewall. After this comes the rule stating that all outgoing internal communications are allowed, followed by the rules governing access to the SMTP server, and denial of Ping, Telnet access, and access to the HTTP server. If heavy traffic to the HTTP server is expected, move the HTTP server rule closer to the top, which would expedite rule processing for external communications.

Why isn't there a comparable rule for the 192.168.2.1 subnet? Because this is an un-routeable network, external communications are handled by the NAT server, which maps internal (192.168.2.0) addresses to external (10.10.10.0) addresses. This prevents a hacker from compromising one of the internal boxes and accessing the internal network with it. The exception is the proxy server, which should be very carefully configured. If the organization does not need the proxy server, as in cases where all externally accessible services are provided from machines in the DMZ, then rule #7 is not needed. Note that there are no Ping and Telnet rules. This is because the external firewall filters these external requests out. The last rule, rule#8 provides cleanup.

### 3.11.1 Contenent Filters

**Q14. Explain the utility of content filters in fire wall?**

*Ans :*

Another utility that can contribute to the protection of the organization's systems from misuse and unintentional denial-of-service, and is often closely associated with firewalls, is the **content filter.**

A content filter is software filter-technically not a firewall –that allows administrators to restrict access to content from within a network. It is essentially a set of scripts or programs that restricts user access to certain networking protocols and internet locations, or restricts users from receiving general types or specific examples of Internet content. Some refer to content filters as reverse firewalls, as their primary focus is to restrict internal access to external material. In most common implementation models, the content filter has two components: rating and filtering. The rating is like a set of firewall rules for Web sites, and is common in residential content filters. The rating can be complex, with multiple access control settings for different levels of the organizations, or it can be simple, with a basic allow/ deny scheme like that of a firewall. The filtering is a method used to restrict specific access requests to the identified resources, which may be Web sites, servers or whatever resources the content filter administrator configures. This is sort of a reverse control list (A capability table), in that whereas an access control list normally records a set of users that have access to resources, this control list records resources which the user cannotaccess.

The first types of content filters were systems designed to restrict access to specific Web sites, and were stand –alone software applications. These could be configured in either an exclusive manner. In an exclusive mode,, certain sites are specifically excluded. The problem with this approach is that there may be thousands of Web sites that an organization wants to exclude, and more might be added every hour. The inclusive mode works off a list of sites that are specifically permitted. In order to have a site added to the list, the user must submit a request to the content filter manager, which could be time- consuming and restrict business operations. Newer models of content filters are protocol–based, examining content as it is dynamically displayed and restricting or permitting access based on a logical interpretation of content.

The most common content filters restrict users from accessing Web sites with obvious non-business related material, such as pornography, or deny incoming spam e-mail. Content filters can be small add-on software programs for the home or office, such as Net Nanny or surfControl, or corporate applications, such as the Novell Border manager. The benefit of implementing content filters is the assurance that employees are not distracted by non-business material and cannot waste organizational time and resources. The downside is that these systems require extensive configuration and on-going maintenance to keep the list of unacceptable destination or the source addresses for incoming restricted e-mail up-to-date. Some newer content filtering applications come with a service of downloadable files that update the database of restrictions. These applications work by matching either a list of disapproved or approved Web sites and by matching key content words, such as "nude" and " sex". Creators of restricted content have, of course, realized this and work to bypass the restrictions by suppressing these types of trip words, thus creating additional problems for networking and security professionals.

### 3.11.2 Protecting Remote Connnections

**Q15. Write a short notes on**

**(a) Dial-Up**

**(b) RADIUS and TACACS**

**(c) Kerberos security**

*Ans :*

The networks that organizations create are seldom used only by people at that location. When connections are made between one network and another, the connectionsare arranged and managed carefully. Installing such network connections requires using leased lines or other data channels provided by common carriers, and therefore these connections are usually permananet and secured under the requirements of a formal service agreement. But when individuals-whether they be employees from home, contract workers hired for specific assignments, or other workers who are

traveling-seek to connect to an organization's network(s), a more flexible option must be provided. In the past, organization's provided these remote connections exclusively through dial-up services like Remote Authentication Service (RAS).Since the Internet has becomemore wide-spread in recent years, other options such as Virtual Private Networks (VPNs) have become more popular.

### Dial-Up

Before the Internet emerged, organizations created private networks and allowed individuals and other organization's to connect to them using dail-up or leased line connections. The connections between company networks and the Internet use firewalls to safeguard that interface. Although connections via dial-up and leased lines are becoming less popular they are still quite common. And it si a widely held view that these unstructured, dial-up connection points represent a substantial exposure to attack. An attacker who suspects that an organization has dial-up lines can use a device called a war dialer to locate the connection points. A war-dialer is an automatic phone-dialling program that dials every number in a configured range (e.g., 555-1000 to 555-2000), and checks to see if a person , answering machine, or modem picks up. If a modem answers, the war dialer program makes a note of the number and then moves to the next target number. The attacker then attempts to hack into the network via the identified modem connection using a variety of techniques. Dial-up network connectivity is usually less sophisticated than that deployed with internet connections. For the most part, simple username and password schemes are the only means of authentication. However , some technologies such as RADIUS systems, TACAS, and CHAP password systems, have improved the authentication process, and there are even systems now that use strong encryption. Authenticating technologies such as RADIUS, TACAS, Kerberos, and SESAME are discussed below.

### RADIUS and TACACS

RADIUS and TACACS are systems that authenticate the credentials of users who are trying to access an organization's network via a dial-up connection. Typical dial-up systems place the responsibility for the authentication of users on the system directly connected to the modems. If there are multiple points of entry into the dial-up system, this authentication system can become difficult to manage.

The **RADIUS (Remote Authentication Dial-In User Service)** system centralizes the management of user authentication by placing the responsibility for authenticating each user in the central RADIUS server. When a remote access server (RAS) receives a request for a network connection from a dial-up client, it passes the request along with the user's credentials to the RADIUS server. RADIUS then validates the credentials and passes the resulting decision (accept or deny) back to the accepting remote access server. The typical configuration of an RAS system. Similar in function to the RADIUS system is the Terminal Access Controller Access Control System (TACACS). TACACS is another remote access authorization system that is based on a client/server configuration. Like RADIUS, it contains a centralized database, and it validates the user's credentials at this TACACS server. There are three versions of TACACS: TACACS, Extended TACACS, and TACACS+. The original version combines authentication and authorization services. The extended version separates the steps needed to provide authentication of the individual or system attempting access from the steps needed to authorize that the authenticated individual or system is able to make this type of connection. The extended version then keeps records that show that the action of granting access has accountability and that the access attempt is linked to a specific individual or system. The plus version uses dynamic passwords and incorporates two-factorauthentication.

### Securing Authentication with Kerberos

Two authentication systems can be implemented to provide secure third-party authentication: Kerberos and Sesame. Kerberos-named after the three-headed dog of Greek mythology (spelled Cerberus in Latin), which guarded the gates to the underworld- uses symmetric key encryption to validate an individual user to various network resources.

Kerberos keeps a database containing the private keys of clients and servers-in the case of a

client, this key is simply the client's encrypted password. Network services running on servers in the network register with Kerberos, as do the clients that use those services. The Kerberos system knows these private keys and can authenticate one network node (client or server) to another. For example, Kerberos can authenticate a user once-atthe time the user logs in to a client computer-and then, at a later time during that session, it can authorize the user to have access to a printer without requiring the user to take any additional action. Kerberos also generates temporary session keys, which are private keys given to the two parties in a conversation. The session key is used to encrypt ali communications between these two parties. Typically a user logs into the network, is authenticated to the Kerberos system, and is then authenticated to other resources on the network by the Kerberos system itself.

Kerberos consists of three interacting services, all of which use a database library:

1. Authentication server (AS), which is a Kerberos server that authenticates clients and servers.
2. Key Distribution Center (KDC), which generates and issues sessionkeys.
3. Kerberos ticket granting service (TGS), which provides tickets to clients who request services. In Kerberos a ticket is an identification card for a particular client that verifies to the server that the client is requesting services and that the client is a valid member of the Kerberos system and therefore authorized to receive service. The ticket consists of the client's and network address, a receive services. The ticket validation starting and ending time,and the session key, all, encrypted in the private key of the server from which the client is requesting services.

**Kerberos is based on the following principles:**

- The KDC knows the secret keys of all clients and servers on thenetwork.
- The KDC initially exchanges information with the client and server byusing
- these secretkeys.
- Kerberos authenticates a client to a requested service on a server through TGS and by issuing temporary session keys for communications between the client and KDC, the server and KDC, and the client andserver.
- Communications then take place between the client and server using these Temporary sessionkeys.

Kerberos may be obtained free of charge from MIT at *http://web.mit.edu/is/help/* Kerberos/, but if you use it, be aware of some fundamental problems. If the Kerberos servers are subjected to denial-of-service attacks, no client can request services. If the Kerberos servers, service providers, or clients' machines are compromised, their private key information may also be compromised.

**Sesame**

The Secure European System for Applications in a Multivendor Environment (SESAME) is the result of a European research and development project partly funded by the European Commission. SESAME is similar to Kerberos in that the user is first authenticated to an authentication server and receives a token. The token is then presented to a privilege attribute server (instead of a ticket granting service as in Kerberos) as proof of identity to gain a privilege attribute certificate(PAC).The PAC is like the ticketing in Kerberos;however, a PAC conforms to the standards of the European Computer Manufacturers Association (ECMA) and the International Organization for Standardization/ International Telecommunications Union (ISO/ITU-T). The balances of the differenceslie in the security protocols and distribution methods used. SESAME uses public key encryption to distribute secretkeys.

SESAME also builds on the Kerberos model by adding additional and more sophisticated access control features, more scalable encryption systems, as well as improved manageability auditing features, and the delegation of responsibility for allowing access.

## 3.12 VIRTUAL PRIVATE NETWORK(VPNS)

**Q16. Write short notes on VPNs.**

*Ans :*

Virtual Private Networks are implementations of cryptographic technology (which you learn about in Chapter 8 of this book). A Virtual Private Network (VPN) is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network. The Virtual Private Network Consortium (VPN (*www.vpnc.org)* defines a VPN as "a private data network that makes use of the Public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. VPNs are commonly used to extend securely an organization's internal network connections to remote locations beyond the trustednetwork.

The VPNC defines three VPN technologies: trusted VPNs, secure VPNs, and hybrid VPNs A trusted VPN, also known as legacy VPN, uses leased circuitsfrom a service provider and conducts packet switching over these leased circuits . The organization must trust the service provider, who provides contractual assurance that no one else is allowed to use these circuits and that the circuits are properly maintained and protected- hence the name *trusted* VPN. Secure VPNs use security protocols and encrypt traffic transmitted across unsecured public networks like the internet. A hybrid VPN combines the two providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPNnetwork.

A VPN that proposes to offer a secure and reliable capability while relying on public networks must accomplish the following, regardless of the specific technologies and protocols being used:

- Encapsulating of incoming and outgoing data, wherein the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network as well as be usable by the server networkenvironment.
- Encryption of incoming and outgoing data to keep the data contents private while in transit over the public network but usable by the client and server computers and/or the local networks on both ends of the VPNconnection.
- Authentication of the remote computer and, perhaps, the remote user aswell.
- Authentication and the subsequent authorization of the user to perform specific options are predicated on accurate and reliable identification of the remote system and/oruser.

In the most common implementation, a VPN allows a user to turn the Internet in private network. As you know, the Internet is anything but private. However, using the tunneling approach an individual or organization can set up tunneling points across the Internet and send encrypted data back and forth, using the IP-packet-within-an-IP-packet method to transmit data safely and securely. VPNs aresimple to set up and maintain usually require only that the tunneling points be dual-horned-that is, connecting a private network to the Internet or to another outside connection point. There is VPN support built into most Microsoft server software, including NT and 2000, as well as client support for VPN services built into XP. While true private network services connections can cost hundreds of thousands of dollars to lease, configure, and maintain, a VPN can cost next nothing. There are a number of ways to implement a VPN. IPSec, the dominant protocol used in VPNs, uses either transport mode or tunnel mode. IPSec can be used as a stand alone protocol, or coupled with the Layer 2 Tunneling Protocol(L2TP).

**Transport Mode**

In transport mode, the data within an IP packet is encrypted) but the header information is not. This allows the user to establish a secure link directly with the remote host, encrypting only the data contains of the packet. The downside to this implementation is that packet eavesdroppers can still determine the destination system. Once an attacker knows the destination, he or she may be able to compromise one of the end nodes and acquire the packet information from it. On the other hand, transport mode eliminates the need for special servers and tunneling software, and allows the end users to transmit traffic from anywhere. This is especially useful for traveling or telecommuting employees.

There are two popular uses for transport mode VPNs . The first is the end-to-end transport of encrypted data. In this model, two end users can communicatedirectly, encrypting and decrypting their communications as needed. Each machine acts as the end node VPN server and client In the second, a remote access worker or teleworker connects to an office network over the Internet by connecting to a VPN server on the perimeter. This allows the teleworker's system to work as if it were part of the local area network. The VPN server in this example acts as on intermediate node, encrypting traffic from the secure intranet and transmitting it to the remote client, and decrypting traffic from the remote client and transmitting it to its finaldestination.

This model frequently allows the remote system to act as its own VPN server, which is a weakness, since most work-at-home employees are not provided with the same level of physical and logical security they would be if they worked in the office.

UNIT IV

**Security Technology:** Intrusion detection, access control and other security **Tolls:** Intrusion detection and prevention systems, Scanning and analysis tools, Access control devices.

**Cryptography:** Foundations of cryptology, Cipher methods, Cryptographic Algorithms, Cryptographic tools, Protocols for secure communications, Attacks on cryptosystems.

## 4.1 Security Technology Intrusion Detection, Access Control and other Security Tools

**Q1. What is intrusion detection system? Explain different reasons and terminology associated.**

*Ans :*

**Introduction**

The discussion on the physical design of an information security program by covering firewalls, dial-up protection mechanisms, content filtering, and VPNs. This chapter builds on that discussion by describing some other technologies-namely, intrusion detection systems; honey pots, honey nets, and padded cell systems; scanning and analysis tools; and access control-that organizations can use to secure their information assets.The fact that information security is a discipline that relies on people in addition to technical controls to improve the protection of an organization's information assets cannot be overemphasized.

In order to understand the technologies discussed, especially intrusion detection systems, you must first understand the nature of the event they attempt to detect. An intrusion is a type of attack on information assets in which the Instigator attempts to gain entry into a system or disrupt the normal operations of a system with, almost always, the intent to do malicious harm. Even when such attacks are self-propagating, as in the case of viruses and distributed denial of services, they were almost always instigated by an individual whose purpose is to, harm an organization. Often, the difference between types of intrusions lies with the attacker: some intruders don't care which organizations they harm and prefer to remain anonymous, while others, like Mafiaboy, crave the notoriety associated with breaking in.

Incident response is the identification of, classification of, response to, and recovery from an incident. The literature in the area of incident response discusses the subject in terms of prevention, detection, reaction, and correction. Intrusion prevention consists of activities that seek to deter an intrusion from occurring. Some important intrusion prevention activities are writing and implementing good enterprise information security policy, planning and performing effective information security programs, installing and testing technology-based information security counter measures, and conducting and measuring the effectiveness of Employee training and awareness activities.

This includes the mechanisms an organization implements to limit the number of false positive alarms while ensuring the detection of true intrusion events. Intrusion reaction encompasses the actions an organization undertakes when an intrusion event is detected. These actions seek to limit the loss from an intrusion and initiate procedures for returning operations to a normal state as rapidly as possible. Intrusion correction activities finalize the restoration of operations to a normal state, and by seeking to identify the source and method of the intrusion in "order to ensure that the same type of attack cannot occur again, they return to intrusion prevention-thus closing the incident response loop.

In addition to intrusion detection systems, this chapter also covers honey pots and padded cell systems, scanning and analysis tools, and access control technologies. Honey pots and padded cell

systems are mechanisms used to attempt to channel or redirect attackers whereas the intrusion detection systems record their actions and notify the system owner. In order to understand how attackers take advantage of network protocol and system weaknesses, you must learn about the specialized scanning and analysis tools they use to detect these weaknesses. The first line of defense against all attackers is an understanding of the basic access control technology built into informationsystems.

**Intrusion Detection Systems (IDSs)**

Information security intrusion detection systems (IDSs) were first commercially available in the late 1990s. An IDS works like a burglar alarm in that it detects a violation of its configuration (analogous to an opened or broken window) and activates an alarm. This alarm can be audible and/or visual (producing noise and lights, respectively), or it can be silent (taking the form of an e-mail message or pager alert). With almost all IDSs, system administrators can choose the configuration of the various alerts and the associated alarm levels for each type of alert. Many IDSs enable administrators to configure the systems to notify them directly of trouble via e-mail or pagers. The systems can also be configured-again like a burglar alarm-to notify an external security service organization of a "break-in." The configurations that enable IDSs to provide such customized levels of detection and response are quite complex. A valuable source of information for more detailed study about IDS is National Institute of Standards and Technology (NIST) Special Publication 800-31, "Intrusion Detection Systems;' written by Rebecca Bace and Peter Mell and available through the NISI's Computer Security Resource Center at http://csrc.nist.gov.

**4.1.1 IDS Terminology**

In order to understand IDS operational behavior, you must first become familiar with some terminology that is unique to the field of IDSs. The following is a compilation of relevant IDS- related terms and definitions that were drawn from the marketing literature of a well-known information security company, TruSecure, but are representative across the industry:

- **Alert or Alarm:** An indication that a system has just been attacked and/or continues to be under attack. IDSs create alerts of alarms to notify administrators that an attack is or was or occurring and may have been successful. Alerts and alarms may takethe form of audible signals, e-mail messages, pager notifications, pop-up windows, or log entries (these are merely written, i.e., they do not involve taking anyaction).
- **False Attack Stimulus:** An event that triggers alarms and causes a false positive when no actual attacks are in progress. Testing scenarios that evaluate the configuration of IDSs may use false attack stimuli to determine if the IDSs can distinguish between these stimuli and real attacks. **False Negative:** The failure of an IDS system to react to an actual attack event. Of all failures, this is the most grievous, for the very purpose of an IDS is to detect attacks.
- **False Positive:** An alarm or alert that indicates that an attack is in progress or that an attack has successfully occurred when in fact there was no such attack. A false positive alert can sometimes be produced when an IDS mistakes normal system operations/activity for an attack. False positives tend to make users insensitive to alarms, and will reduce their quickness and degree of reaction to actual intrusion events through the process of desensitization to alarms and alerts. This can make users less inclined, and therefore slow, to react when an actual intrusionoccurs.
- **Noise:** The ongoing activity from alarm events that are accurate and noteworthy but not necessarily significant as potentially successful attacks. Unsuccessful attacks are the most common source of noise in IDSs, and some of these may not even be attacks at all, but rather employees or the other users of the local network simply experimenting with scanning and enumeration tools without any intent to do harm. The issue faced regarding noise is that most of the intrusion events detected are not malicious and have no significant chance of causing a loss.
- **Site Policy:** The rules and configuration guidelines governing the implementation and operation of IDSs within the organization.

- **Site Policy Awareness**: An IDSs ability to dynamically modify its site policies in reaction or response to environmental activity. A so-called Smart ID can adapt its reaction activities based on both guidance learned over the time from the administrator and circumstances present in the local environment. Using a device of this nature, the IDs administrator acquires logs of events that fit a specific profile instead of being alerted about minor changes, such as when a file is changed or a user login fails. Another advantage of using a Smart IDS is that the IDS knows when it does not need to alert the administrator-this would be the case when an attack using a known and documented exploit is made against systems that the IDS knows are patched against that specific kind of attack. When the IDS can accept multiple response profiles based on changing attack scenarios and environmental values, it can be made much moreuseful.
- **True Attack Stimulus:** An event that triggers alarms and causes an IDS to react as if a real attack is in progress. The event may be an actual attack, in which an attacker is at work on a system compromise attempt, or it may be a drill, in which security personnel are using hacker tools to conduct tests of a network segment.
- **Confidence Value:** A value associated with an IDS's ability to detect and identify an attack correctly. The confidence value an organization places in the IDS is based on experience and past performance measurements. The confidence value, which is a type of fuzzy logic, provides an additional piece of information to assist the administrator in determining whether an attack alert is indicating that an actual attack in progress, or whether the IDS is reacting to false attack stimuli and creating a false positive. For example, if a system deemed capable of reporting a denial-of-service attack with 90% confidence sends an alert, there is a high probability that an actual attack isoccurring.
- **Alarm Filtering:** The process of classifying the attack alerts that an IDS produces in order to distinguish/sort false positives from actual attacks more efficiently. Once anIDS has been installed and configured, the administrator can set up alarm filtering by first running the system for a while to track what types of false positives it generates and then adjusting the classification of certain alarms. For example, the administrator may set the IDS to discard certain alarms that he or she knows are produced by false attack stimuli or normal network operations. Alarm filters are similar to packet filters in that they can filter items by their source or destination IP addresses, but they have the additional capability of being able to filter by operating systems, confidencevalues, alarm type, or alarm severity.
- **Alarm Clustering:** A consolidation of almost identical alarms into a single higher-level alarm. This consolidation will reduce the total number of alarms generated, thereby reducing administrative overhead, and will also indicate a relationship between the individual alarm elements.
- **Alarm Compaction:** Alarm clustering that is based on frequency, similarity in attack signature, similarity in attack target, or other similarities. Like the previous form of alarm clustering, this will reduce the total number of alarms generated, thereby reducing administrative overhead, and will also indicate a relationship between the individual alarm elements when they have specific similar attributes.

**Why Use an IDS?**

According to the NIST's documentation on industry best practices, there are several compelling reasons to acquire and use an IDS:

1. To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse thesystem
2. To detect attacks and other security violations that are not prevented by other security measures
3. To detect and deal with the preambles to attacks (commonly experienced as network probes and other 'doorknob rattling'activities)

4. To document the existing threat to anorganization.
5. To act as quality control for security design and administration, especially of large and complexenterprises.
6. To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causativefactors.

One of the best reasons why organizations should install an IDS is that these systems can serve as straight forward deterrent measures, by increasing the fear of detection and discovery among would-be attackers. If internal and external users know that an organization has an intrusion detection system, they are less likely to probe or attempt to compromise it, just as criminals are much less likely to break into a house that has been clearly marked as having a burglaralarm.

The second reason for installing an 1OS is to cover the organization when its network fails to protect itself against known vulnerabilities or is unable to respond to a rapidly changing threat environment There are many factors that can delay or undermine. An organization's ability to make its systems safe from attack and subsequent loss. For example, even though popular information security technologies such as scanning tools (to be discussed later in this chapter) allow security administrators to evaluate the readiness of their systems, they may still fail to detect or correct a known deficiency, or may perform the vulnerability-detection process too infrequently. In addition, even when a vulnerability is detected in a timely manner, it cannot always be corrected quickly. Also, because such corrective measures usually involve the administrator installing patches and upgrades, they are subject to delays caused by fluctuation in the administrator's workload. To further complicate the matter, sometimes there are services that are known to be vulnerable, but they are so essential to ongoing operations that they cannot be disabled or otherwise protected in the short term. At such times-that is, when there is a known vulnerability or deficiency in the system-an IDS can be particularly effective, as it can be set up to detect attacks or attempts to exploit existing weaknesses. By, in effect, guarding these vulnerabilities, IDS can become an important part of the strategy of defense in depth.

The next reason why IDSs are useful is that they can help administrators detect the preambles to attacks. Most attacks begin with an organized and thorough probing of the organization's network environment and its defenses. This initial estimation of the defensive state of an organization's networks and systems is called doorknob rattling and is conducted first through activities collectively known as foot printing (which involves gathering information about the organization and its network activities and the subsequent process of identifying network assets), and then through another set of activities collectively known as fingerprinting (in which network locales are scanned for active systems, and then the network services offered by the host systems on that network are identified). When a system is capable of detecting the early warning signs of foot printing and fingerprinting, much as neighborhood watch volunteers might be capable of detecting potential burglars who ale casing their neighborhoods by skulking through and testing doors and windows, then the administrators may have time to prepare for a potential attack or to take actions to minimize potential losses from anattack.

A fourth reason for acquiring an IDS is documentation. In order to justify the expenses associated with implementing security technology like an IDS (and other controls such as firewalls), security professionals frequently have to make a business case. Since projects to deploy these technologies are often very expensive, almost all organizations require that project proponents

document the threat from which the organization must be protected. The most frequent method used for doing this is to collect data on the attacks that are currently occurring in the organization and other similar organizations. While such data can be found in published reports or journal articles, first-hand measurements and analysis of the organization's own local network data are likely to be the most persuasive. As it happens, one means of collecting such data is by using IDS. Thus, IDSs are self-justifying systems-that is, they can serve to document the scope of the threat(s) an organization faces and thus produce data that can help administrators persuade management that additional expenditures in information security technologies (e.g., IDSs) are not only warranted, but critical for the ongoing protection of information assets. Measuring attack information with a freeware IDS tool (such as snort) may be a way to begin this process of docume-ntation.

Another reason that supports the use of an IDS relates to the concepts of quality assurance and continuous improvement, which are both we!! known to most senior managers. In terms of quality control, IDSs support the concept of defense in depth, for they can consistently pick upinformation about attacks that have successfully compromised the outer layers of information security controls—that is, compromised controls such as a firewall. This information can be used to identify and repair emergent or residual flaws in the security and network architectures, and thus help the organization expedite its incident response process and make other such continuous improvements.

A final reason for installing an IDS is that even if an IDS fails to prevent an intrusion, it can still assist in the after-attack review by helping a system administrator collect information on how the attack occurred, what the intruder accomplished, and which methods the attacker employed. This information can be used, as discussed in the preceding paragraph, to remedy deficiencies as well as trigger the improvement process to prepare the organization's network environment for future attacks. The IDS may also provide forensic information that may be useful as evidence, should the attacker be caught and criminal or civil legal proceedings pursued. In the case of handling forensic information, an organization should follow commonly accepted and legally mandated procedures for handling evidence. Foremost among these is that the information collected should be stored in a location and manner that precludes its subsequent modification. Other legal requirements and plans the organization has for the use of the data may warrant additional storage and handling constraints. As such, an organization may find it useful to consult with legal counsel when determining policy governing this situation.2

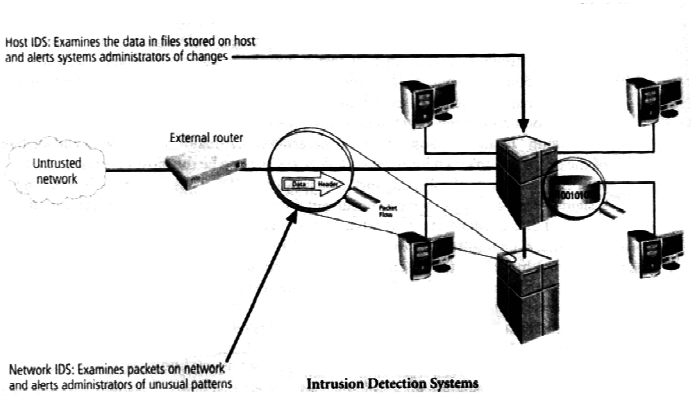


## 4.2 Types of IDSs and Detection Methods

**Q2. What are the different types of intrusion detection system avaliable? Explain with read diagram?**

*Ans :*

IDS's operate as network-based, host-based, or application-based systems. A network-based !OS is focused on protecting network information assets. A host -based version is focused on protecting the server or host's information assets. example that monitors both network connection activity and current information states on host servers. The application- based model works on one or more host systems that support a single application and is oriented to defend that specific application from special forms of attack. Regardless of whether they operate at the network, host, or application level, all IDSs use one of two detection methods: signature-based or statistical anomaly-based. Each of these approaches to intrusion detection is examined in detail in the following sections.



Intrusion Detection Systems

## Network-Based IDS

A **network-based IDS (NIDS)** resides on a computer or appliance connected to a segment of an organization's network and monitors network traffic on that network segment, looking for indications of ongoing or successful attacks. When a situation occurs that the NIDS is programmed to recognize as an attack, it responds by sending notifications to administrators. When examining the packets "transmitted through an organization's networks, a NIDS looks for attack patterns within network traffic such as large collections of related items that are of a certain type, which could indicate that a denial-of service attack is underway, or the exchange of a series of related packets in a certain pattern, which could indicate that a port scan is in progress. A NIDS can detect many more types of attacks than a host-based IDS, but to do so, it requires a much more complex configuration and maintenanceprogram.

A NIDS is installed at a specific place in the network (such as on the inside of an edge router) from where it is possible to watch the traffic going into and out of a particular network segment. The NIDS can be deployed to watch a specific grouping of host computers on a specific network segment, or it may be installed to monitor all traffic between the systems that make up an entire network. When placed next to a hub, switch, or other key networking device, the NIDS may use that device's monitoring port. The monitoring port, also known as a switched port analysis (SPAN) port or mirror port, is a specially configured connection on a network device that is capable of viewing all of the traffic that moves through the entire device. In the early '90s, before switches became the popular choice for connecting networks in a shared-collision domain, hubs were used. Hubs received traffic from one node, and retransmitted it to all other nodes. This configuration allowed any device connected to the hub to monitor all traffic passing through the hub. Unfortunately, it also represented a security risk, since anyone connected to the hub could monitor all the traffic that moved through that network segment. More recently, switches have been deployed on most networks, and they, unlike hubs, create dedicated point-to-point links between their ports. These links create a higher level of transmission security and privacy, and effectively prevent anyone from being able to capture, and thus eavesdrop on, the traffic passing through the switch. Unfortunately, however, this ability to capture the traffic is necessary for the use of an IDS. Thus, monitoring ports are required. These connections enable network administrators to collect traffic from across the network for analysis by the IDS as well as for occasional use in diagnosing network faults and measuring network performance.

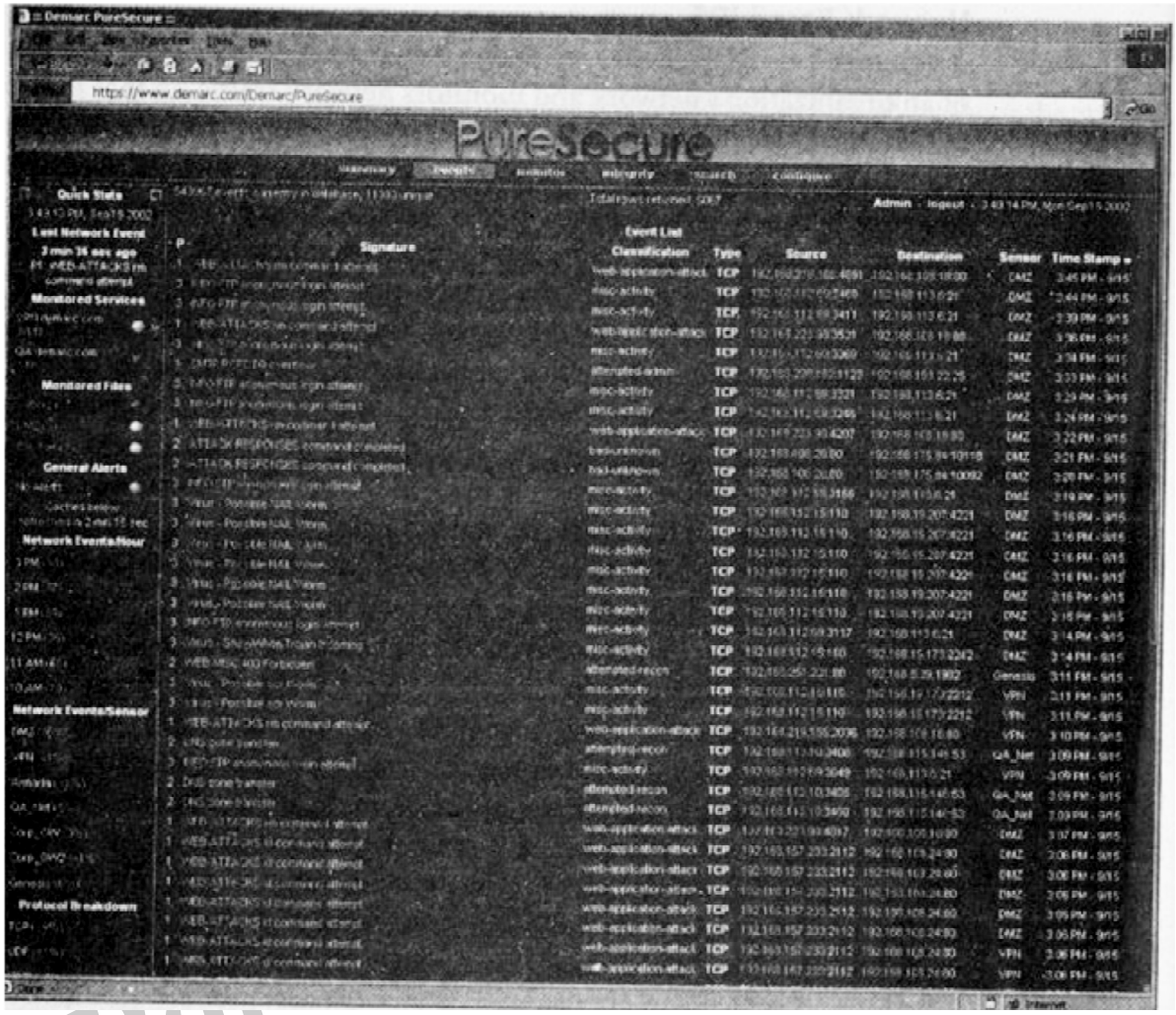



**Fig: Demarc Pure Secure Total Intrusion Detection**

**NIDS Signature Matching:** To determine whether or not an attack has occurred or may be underway, NIDSs must look for attack patterns by comparing measured activity to known signatures in their knowledge base. This is accomplished by the comparison of cap turned network traffic using a special implementation of the TCP/IP stack that reassembles the packets and applies protocol stack verification, application protocol verification, and/or other verification and comparison techniques.

In the process of protocol stack verification, the NIDSs look for invalid data packets i.e., packets that are malformed under the rules of the TPC/IP protocol A data packet is verified when its configuration matches that defined by the various Internet protocols (e.g., TCP, UDP, IP). The elements of the protocols in use (IP, TCP, UDP, and application layers such as HTTP) are combined in a complete set called the protocol stack when the software is implemented in an operating system or application. Many types of intrusions, especially DoS and DDoS attacks, rely on the creation of improperly formed packets to take advantage of weaknesses in the protocol stack in certain operating systems orapplications.

In application protocol verification, the higher-order protocols (e.g., HTTP, FTP, Telnet) are examined for unexpected packet behavior, or improper use. Sometimes an intrusion involves the arrival of valid protocol packets but in excessive quantities (in the case of the Tiny Fragment Packet attack, the packets are also excessively fragmented).

While the protocol stack verification looks for violations in the protocol packet structure, the application protocol verification looks for violations in the protocol packet use. One example of this kind of attack is DNS cache poisoning, in which valid packets exploit poorly configured DNS servers to inject false information to corrupt the servers' answers to routine DNS queries from other systems on the network. Unfortunately, however, this higher-order examination of traffic can have the same effect on an IDSas it can on a firewall-that is, it slows the throughput of the system. As such, it may be necessary to have more than one NIDS installed, with one of them performing protocol stack verification and one performing application protocol verification.

**Advantages and Disadvantages of NIDSs:** The following is a summary, taken from Bace and Mell, of the advantages and disadvantages of NIDSs:

**Advantages:**

1. Good network design and placement of NIDS devices can enable an organization to use a few devices to monitor a largenetwork.
2. NIDSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal networkoperations.
3. NIDSs are not usually susceptible to direct attack and, in fact, may not be detectable by attackers.

**Disadvantages:**

1. A NIDS can become overwhelmed by network volume and fail to recognize attacks it might otherwise have detected. Some IDS vendors are accommodating the need for ever faster network performance by improving the processing of detection algorithms in dedicated hardware circuits to gain a performance advantage. Additional efforts to optimize rule set processing may also reduce overall effectiveness in detecting attacks.
2. NIDSs require access to all traffic to be monitored. The broad use of switched Ethernet networks has replaced the ubiquity of shared collision domain hubs. Since many switches have limitedornomonitorin gportcapability, some networks are not capable of providingaggregate data for analysis by a NIDS. Even when switches do provide monitoring ports, they may not be able to mirror aJl activity with a consistent and reliable time sequence.
3. NIDSs cannot analyze encrypted packets, making some of the network traffic invisible to the process. The increasing use of encryption that hides the contents of some or all of the packet by some network services (such as SSL, SSH, and VPN) limits the effectiveness ofNIDSs.
4. NIDSs cannot reliably ascertain if an attack was successful or not. This requires the network administrator to be engaged in an ongoing effort to evaluate the results of the lugs of suspicious networkactivity.
5. Some forms of attack are not easily discerned by NIDSs, specifically those involving fragmented packets. In fact, some NIDSs are particularly susceptible to malformed packets and may become unstable and stop functio-ning.4

**Host-Based IDS**

A host-based IDS (HIDS) works differently from a network-based version of IDS. While a network-based IDS resides on a network segment and monitors activities across that segment, a host-based IDS resides on a particular computer or server, known as the host, and monitors activity only on that system. HIDSs are also known as system integrity verifier as they benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files. A HIDS is also capable of monitoring system

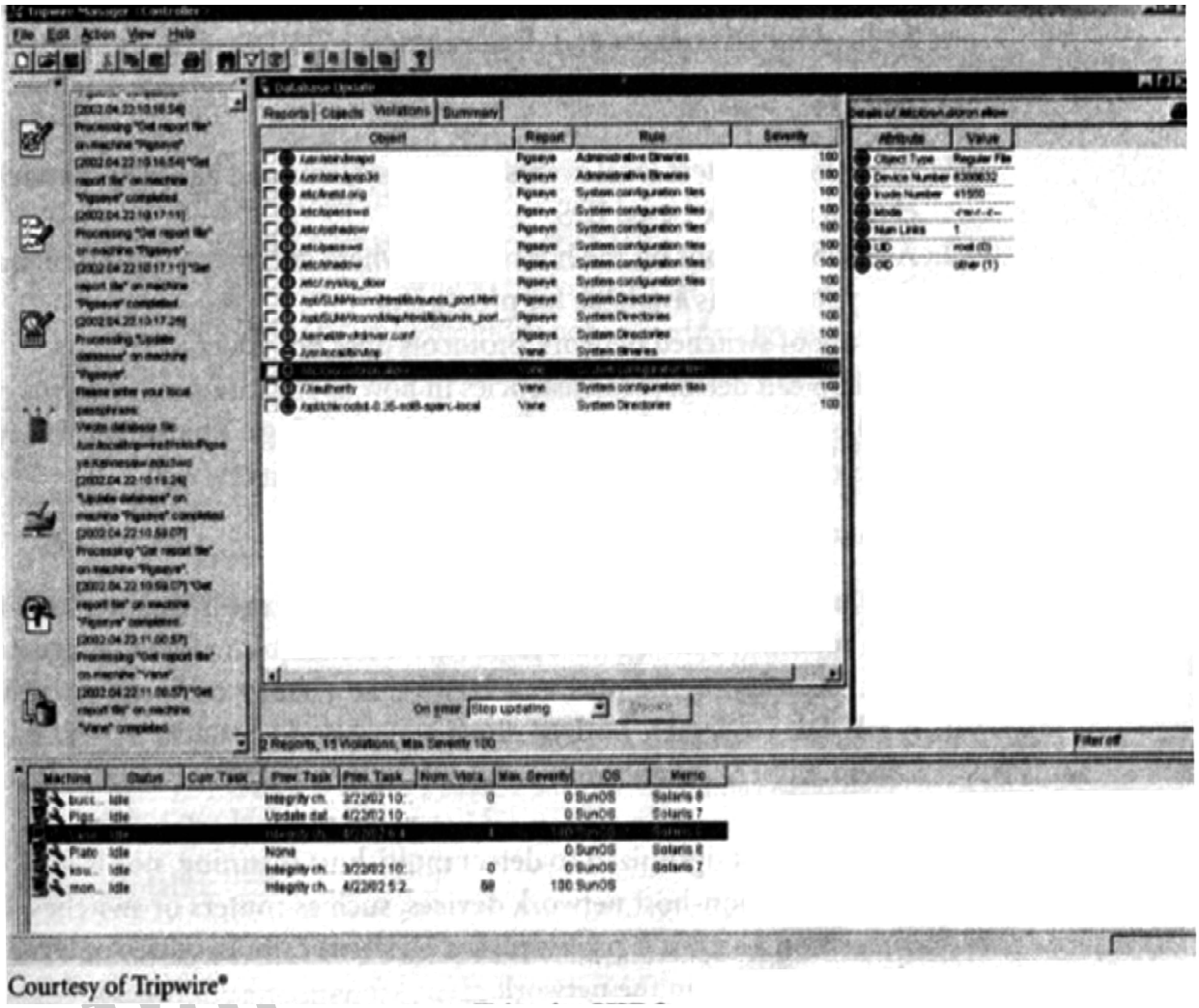
configuration databases, such as Windows registries, in addition to stored configuration files like .ini, .cfg, and.dat files. Most HIDSs work on the principle of configuration or change management, which means they record the sizes, locations, and other attributes of system files. The HIDS then triggers an alert when one of the following changes occurs: file attributes change, new files are created, or existing files are deleted. A HIDS can also monitor systems logs for predefined events. The HIDS examines these files and logs to determine if an attack is Underway or has occurred, and if the attack is succeeding or was successful. The HIDS will maintain its own log file so that even when hackers successfully modify files on the target system to cover their tracks, the HIDS can provide an independent audit trail of theattack.

Once properly configured, a HIDS is very reliable. The only time a HIDS produces a false positive alert is when an authorized change occurs for a monitored file. This action can be quickly reviewed by an administrator and dismissed as acceptable. The administrator may choose then to disregard subsequent changes to the same set of files. If properly configured, a HIDS can also detect when an individual user attempts to modify or exceed his or her access authorization and give him or herself higher privileges.

A HIDS has an advantage over NIDS in that it can usually be installed in such a way that it can access information that is encrypted when traveling over the network. For this reason, a HIDS is able to use the content of otherwise encrypted communications to make decisions about possible or successful attacks. Since the HIDS has a mission to detect intrusion activity on one computer system, all the traffic it needs to make that decision is coming to the system where the HIDS is running. The nature of the network packet delivery, whether switched or in a shared-collision domain, is not a factor.

A HIDS relies on the classification of files into various categories and then applies various notification actions, depending on the rules in the HIDS configuration. Most HIDSs provide onlya few general levels of alert notification. For example, an administrator can configure a HIDS to treat the following types of changes as reportable security events: changes in a system folder (e.g., in C:\Windows or C:\WINNT); and changes within a security-related application (such as C:\TripWire). In other words, administrators can configure the system to alert on any changes within a critical data folder. The configuration rules may classify changes to a specific application folder (e.g., C:\Program Files\Office) as being normal, and hence unreportable. Administrators can configure the system to log all activity but to page them or e-mail them only if a reportable security event occurs. Although this change-based system seems simplistic, it seems to suit most administrators, who, in general, become concerned only if unauthorized changes occur in specific and sensitive areas of the host file system. Applications frequently modity their internal files, such as dictionaries and configuration templates, and users are constantly updating their data files. Unless a HIDS is very specifically configured, these actions can generate a large volume of falsealarms.

Managed HIDSs can monitor multiple computers simultaneously. They do this by creating a configuration file on each monitored host and by making each HIDS report back to a master console system, which is usually located on the system administrator's computer. This master console monitors the information provided from the managed hosts and notifies the administrator when it sense's recognizable attack conditions.




**Tripwire HIDS**

In configuring a HIDS.the system administrator must begin by identifying and categorizing folders and files. One of the most common methods is to designate folders using a pattern of red, yellow, and green categories. Critical systems components are coded red, and usually include the system registry and any folders containing the OS kernel, and application software. Critically important data should also be included in the red category. Support components, such as device drivers and other relatively important files, are generally coded yellow; and user data is usually coded green. This is not to suggest that user data is unimportant, but in practical and strategic terms, monitoring changes to user data does have a lower priority. One reason for this is that users are often assigned storage space that they are expected to use routinely to maintain and back up their documents, files, and images; another reason is that user data files are expected to change frequently-that is, as users make modifications. Systems kernel files, on the other hand, should only change during upgrades or installations. Categorizing critical systems components at a different level from less important files will ensure that the level of response to change will be in proportion to the level of priority. Should the three-tier system be overly simplistic for an organization, there are systems that allow for an alternative scale of 0-100, with 100 being most mission-critical and zero being unimportant. It is not unusual, however, for these types of scales to be overly refined and result in confusion regarding, for example, the prioritization of responses to level 67 and 68 intrusions. Sometimes simpler is better.

**Advantages and Disadvantages of HIDSs:** The following is a summary, taken from Bace and Mell, of the advantages and disadvantages of HIDSs:

**Advantages:**

1. A HIDS can detect local events on host systems and also detect attacks that may elude a network-basedIDS.
2. A HIDS functions on the host system, where encrypted traffic will have been decrypted and is available forprocessing.
3. The use of switched network protocols does not affect aHIDS.
4. A HIDS can detect inconsistencies in how applications and systems programs were used by examining the records stored in audit logs. This can enable it to detect some types of attacks, including Trojan Horse programs.

**Disadvantages:**

1. HIDSs pose more management issues since they are configured and managed on each monitored host. This means that it will require more management effort to install, configure, and operate a HIDS than a comparably sized NIDS solution.
2. A HIDS is vulnerable both to direct attacks and to attacks against the host operating system. Either circumstance can result in the compromise and/or loss of HIDSfunctionality.
3. A HIDS is not optimized to detect multi-host scanning, nor is it able to detect the scanning of non-host network devices, such as routers or switches. Unless complex correlation analysis is provided, the HIDS will not be aware of attacks that span multiple devices in the network.
4. A HIDS is susceptible to some denial-of-service attacks.
5. A HIDS can use large amounts of disk space to retain the host as audit logs; and to function properly, it may require disk capacity to be added to thesystem.
6. A HIDS can inflict a performance overhead on its host systems, and in some cases may reduce system performance below acceptable levels.

**Application-Based IDS**

A refinement of the host-based IDS is the application-based IDS (App IDS). Whereas the HIDS examines a single system for file modification, the application-based IDS examines an application for abnormal events. It usually does this examination by looking at the. files created by the application and looking for anomalous occurrences such as users exceeding their authorization, invalid file executions, or other activities that would indicate that there is a problem in the normal interaction between the users, the application, and the data. By tracking the interaction between users and applications, the App IDS is able to trace specific activity back to individual users. One unique advantage of the App IDS is its ability to view encrypted data. Since the App IDS interfaces with data as it is processed by an application, and any encrypted data that enters an application is decrypted by the application itself, an App IDS does not need to become involved in the decryption process. This allows an App IDS to examine the encryption/decryption process and identity any potential anomalies in data handling or user access.

According to the Missouri State Information Infrastructure Protection Agency, "application- based IDS may be configured to intercept the following types of requests and use them in combinations and sequences to constitute an application's normal behavior:

- File System (file read or write)
- Network (packet events at the driver (NDIS) or transport (TDI) level) Configuration (read or write to the registry on Windows)
- Execution Space (write to memory not owned by the requesting application; for example, attempts to inject a shared library DLL into another process).

Advantages and Disadvantages of App IDS. The following is a summary, taken from Bace and Mell. of the advantages and disadvantages of App IDSs:

**Advantages:**

1. An App IDS is aware of specific users and can observe the interaction between the Application and the user. This allows the App IDS to attribute unauthorized activities to specific and knownusers.
2. An App IDS is able to operate even when incoming data is encrypted since it is able to operate at the point in the process when the data has been decrypted by applications and has not been re- encrypted for storage.

**Disadvantages:**

1. App IDSs may be more susceptible to attack than other IDS approaches, since applications are often less well protecte Ciha; network and first ascomponents.
2. App IDSs are less capable of detecting software tampering and may be taken in by Trojan Horse code or other forms of spoofing, It is usually recommended that App IDS be used in combination with "HIDS andNIDS.

**Signature-Based IDS**

The preceding sections described where the IDS system should be placed for the purpose of monitoring a network, a host, 0r an application Another important differentiation among IDSs is based on detection methods-in other words, on how the IDS should make decisions about intrusion activity. Two detection methods dominate: the signature-based approach and the statistical-anomaly approach. A signature-based IDS (sometimes called a knowledge-based IDS) examines data traffic in search of patterns that match known signatures-that is, preconfigured, predetermined attack patterns. Signature-based IDS technology is widely used because many attacks have clear and distinct signatures, for example: 1 foot printing and fingerprinting activities, described in detail earlier in this chapter, have an attack pattern that Includes the use of ICMP, DNS querying, and e-mail routing analysis; (2) exploits involve a specific attack sequence designed to take advantage of a vulnerability to gain access to a system; (3) denial-of- service (DoS) and distributed denial-of-service (DDoS) attacks, during which the attacker tries to prevent the normal usage of a system, entail over loading the system with requests so that the system's ability to process them efficiently is compromised/ disrupted and it begins denying services to authorizedusers.

The problem with the signature-based approach is that as new attack strategies are identified the IDS's database of signatures must be continually updated. Failure to keep this database current can allow attacks that use new strategies to succeed. An IDS that uses signature-based methods works in ways much like most antivirus software. In fact, antivirus software is often classified as a form of signature-based IDS. This is why experts tell users that if they don't keep their antivirus software updated, it will nor work as effectively. Another weakness of the signature- based method is the time frame over which attacks occur. If attackers are purposefully slow and methodical, they may slip undetected through this type of IDS because their actions will not match those of their signatures, which often include the time allowed between steps in the attack. The only way for a signature-based IDS to resolve this vulnerability is for it to collect and analyze data over longer periods of time, a process that requires substantially larger data storage capability and additional processingcapacity.

**Statistical Anomaly-Based IDS**

Another approach for detecting intrusions is based on the frequency with which certain network activities take place. The statistical anomaly-based IDS(stat-IDS) or behavior-based IDS collects statistical summaries by observing traffic that is known to be normal. This normal period of evaluation establishes a performance baseline. Once the baseline is established, the stat IDS will periodically sample network activity, and, using statistical methods, compare the sampled network activity to this baseline. When the measured activity is outside the baseline parameters, it is said to exceed the clipping level; at this point, the IDS will trigger an alert to notify the administrator. The data that is measured from the normal traffic used to prepare the baseline can include variables such as host memory or CPU usage, network packet types, and packet quantities. Them e asured activity is considered to be outside the base line parameters (and thus will trigger an alert) when there is an anomaly, or inconsistency, in the comparison of these variables.

The advantage of the statistical anomaly-based approach is that the IDS can detect new types of attacks, for it is looking for abnormal activity of any type. Unfortunately, however, these systems require much more overhead and processing capacity than signature-based ones, as they must constantly compare patterns of activity against the baseline. Another drawback is that these systems may not detect minor changes to system variables and may generate many false positives. If the actions of the users or systems on a network vary widely, with periods of low activity interspersed with periods of frantic packet exchange, this type of IDS may not be suitable, because the dramatic swings from one level to another will almost certainly generate false alarms, Because of its complexity and impact on the overhead computing load of the host computer as well as the number of false positives it can generate, this type of IDS is less commonly used than the signature-basedtype.

## 4.3 Log File Monitors

**Q3. What is file monitoring? Why log management is absolutely critical? how.**

*Ans :*

**A log file monitor (LFM)** is an approach to IDS that is similar to the NIDS. Using LFM, the system reviews the log files generated by servers, network devices, and even other IDSs. These systems look for patterns and signature in the log files that may indicate that an attack or intrusion is in process or has already succeeded. While an individual host IDS is only able to look at the activity in one system, the LFM is able to look at multiple log files from a number of different systems, The patterns that signify an attack can be subtle and hard to distinguish when one system is examined in isolation, but they may be much easier to identify when the entire network and its systems are viewed holistically. Of course this holistic approach will require the allocation of considerable resources since it will involve the collection, movement, storage, and analysis of very large quantities of logdata.

### IDS Response Behavior

Each IDS will respond to external stimulation in different ways, depending on its configuration and function. Some may respond in active ways, collecting additional information about the intrusion, modifying the network environment, or even taking action against the intrusion. Others may respond in positive ways, setting off alarms or notifications, collecting passive data through SNMP traps, and the like.

### Response Options for an IDS

Once an IDS detects an anomalous network situation, it has a number of options, depending on the policy and objectives of the organization that has configured it as well as the capabilities of the organization's system, In configuring an IDS's responses to alerts, the system administrator must exercise care to ensure that a response to an attack (or potential attack) does not compound the problem or create a situation that is more disastrous than that of a successful attack. For example, if a NIDS reacts to a suspected DoS attack by severing the network connection, the NIDS has just accomplished what the attacker had hoped. If the attacker discovers that this is the default response to a particular kind of attack, all he or she has to do is repeatedly attack the system at intervals in order to have the organization's own IDS response interrupt its normal business operations. An analogy to this approach would be the case of a potential car thief who walks up to a desirable target in the early hours of a morning, strikes the car's bumper with a rolled up newspaper, and then ducks into the bushes. When the car alarm is triggered, the carowner wakes up, checks the car, determines there is no danger, resets the alarm, and goes back to bed. The thief then repeats the triggering actions every half hour or so until the owner gets so frustrated that he or she disables the alarm, believing it to be malfunctioning. The thief is now free to steal the car without worrying about triggering the alarm.

IDS responses can be classified as active or passive. An active response is one in which a definitive action is initiated when certain types of alerts are triggered. These automated responses include collecting additional information, changing or modifying the environment, and taking action against the intruders. In contrast, IDSs with passive response options simply report the information they have already collected and wait for the administrator to take actions. Generally, the administrator chooses

a course of action after he or she has analyzed the collected data, and thus with passive-response IDSs, the administrator becomes the active component of the overall system. The latter is currently the most common implementation, although most systems allow some active options that are kept disabled by default.

The following list illustrates some of the responses an IDS can be configured to produce. Note that some of these are unique to a network-based or a host-based IDS, while others are applicable to both.

- **Audible / visual alarm:** The IDS can trigger a wav file, beep, whistle, siren, or other audible or visual notification to alert the administrator of an attack. The most common type of such notifications is the computer pop-up window. This display can be configured with color indicators and specific messages, and it can also contain specifics as to what type of attack is suspected, the tools used in the attack, the level of confidence the system has in its own determination, and the addresses and/or locations of the systems involved.
- **SNMP traps and Plug-ins:** The Simple Network Management Protocol contains trap functions, which allow a device to send a message to the SNMP management console to indicate that a certain threshold has been crossed, either positively or negatively. The IDS can execute this trap, telling the SNMP console an event has occurred. Some of the advantages of this operation include the relatively standard implementation of SNMP in networking devices, the ability to configure the network system to use SNMP traps in this manner, the ability to use systems specifically to handle SNMP traffic, including IDS traps, and the ability to use standard communi-cations networks.
- **E-mail message:** The IDS can e-mail an individual to notify him or her of an event. Many administrators use personal digital assistants (PDAs) to check their e-mail frequently, thus have access to immediate global notification. Organizations should use caution in relying on e-mail systems as the primary means of communication between the IDS and security personnel, for not only is e-mail inherently fraught with reliability issues, but an intruder may compromise the e-mail system and block the sending of any such notificationmessages.
- **Page or phone message:** The IDS can be configured to dial a phone number, producing either an alphanumeric page or a modem noise on a phonecall.
- **Log entry:** The IDS can enter information about the event (e.g., addresses, time, systems involved, protocol information, etc.) into an IDS system log file, or operating system log file. These files can be stored on separate servers to prevent skilled attackersfrom deleting entries about their intrusions and thus hiding the details of theirattack.
- **Evidentiary packet dump:** Those organizations that have a need for legal uses of the IDS Data may choose to record all log data in a special way. This method will allow the organization to perform further analysis on the data and also submit the data as evidence in a future civil or criminal case. Once the data has been written using a cryptographic hashing algorithm, it becomes evidentiary documentation-that is, suitable for criminal or civil court use. This packet logging can, however, be resource-intensive, especially in denial-of-serviceattacks.
- **Take action against the intruder:**It has become possible, although not advisable, to take action against an intruder. Known as trap and trace, hack-hacking, or traceback, this response option involves configuring intrusion detection systems to conduct a trace on the data leaving the attacked site and heading to the systems instigating the attacks. The idea here is that once these attacking systems are identified, some form of counterattack can be initiated. While this sounds tempting, it is ill advised and may not be legal. An organization only owns a network to its perimeter, and conducting traces or back-hacking to systems outside that perimeter may make the organization just as criminally liable as the individual(s) who began the attack. In

addition, it is not uncommon for an attacker to compromise an intermediary system and use that system to conduct the attack. If an organization attempts a back-hack and winds up damaging or destroying data on the intermediary system, it has, in effect, attacked an innocent third party, and will therefore be regarded, in the eyes of that party, as an attacker. The matter can be further complicated if the hacker has used address spoofing, a means by which the attacker can freely change the address headers on the source fields in the IP headers and make the destination address recipients think the packets are coming from one location, when in reality they are coming from somewhere else. Any organization planning to configure any sort of retaliation effort into an automated intrusion detection system is strongly encouraged to seek legalcounsel.

- **Launch program:** An IDS can be configured to execute a specific program when it detects specific types of attacks. A number of vendors have specialized tracking, tracing, and response software that could be part of an organization's intrusion responsestrategy.
- **Reconfigure firewall:** An IDS could send a command to the firewall to filter out suspected packets by IP address, port, or protocol. While it may not be easy, an IDS can block or deter intrusions by one of the followingmethods:
  - Establishing a block for all traffic from the suspected attacker's IP address, or even from the entire source network from which the attacker appears to be operating. This blocking might be set for a specific period of time and be reset to normal rules after that period has expired.
  - Establishing a block for specific TCP or UDP port traffic from the suspected attacker's address or source network, blocking only the services that seem to be under attack.
  - Blocking all traffic to or from a network interface (such as the organization's Internet connection) if the severity of the suspected attack warrants that level of response.
  - **Terminate session:** Terminating the session by using the TCP/IP protocol specified packet TCP close is a simple process. Some attacks would be deterred or blocked by session termination, but others would simply continue when the attacker issues a new session request.
  - **Terminate connection:** The last resort for IDS under attack would be to terminate the organization's internal or external connections. Smart switches can cut traffic to/from a specific port, should that connection be linked to a system that is malfunctioning or otherwise interfering with efficient network operations. As indicated earlier, this response should be the last resort to protect information, as it may be the very goal of the attacker.

**Reporting and Archiving Capabilities**

Many, if not all, commercial IDSs provide capabilities to generate routine reports and other detailed information documents. Some of these can output reports of system events and intrusions detected over a particular reporting period.Some provide statistics or logs generated by the IDSs in formats suitable for inclusion in database systems or for use in report generating packages.

**Failsafe Considerations for IDS Responses**

Another factor for consideration when considering IDS architectures and products is the failsafe features included by the design and/or product. Failsafe features are those design features meant to protect the IDSs from being circumvented or defeated by an attacker. These represent a necessary difference between standard system management tools and security management tools. There are several areas that require failsafe measures. For instance, IDSs need to provide silent, reliable monitoring of attackers. Should the response function of an IDS break this silence by broadcasting alarms and alerts in plaintext over the monitored network, it would allow attackers to detect the-presence of the IDS. Worse yet, the attackers can

directly target the IDS as part of the attack on the victim system. Encrypted tunnels or other cryptographic measures used to hide and authenticate IDS communications are excellent ways to secure and ensure the reliability of the IDS.

**Selecting IDS Approaches and Products**

The wide array of intrusion detection products available today addresses a broad range of organizational security goals and considerations. Given that range of products and features, the process of selecting products that represent the best fit for any specific organization's needs is challenging. The following questions may be useful when preparing a specification for acquiring and deploying an intrusion detection product.

**Technical and Policy Considerations**

In order to determine which IDS would best meet the needs of a specific organization's environment, first consider that environment, in technical, physical, and political terms.

**What Is Your Systems Environment?**

The first hurdle a potential IDSmust clear is that of functioning in your systems environment. This is important, for if an IDS is not designed to accommodate the information sources that are available on your systems, it will not be able to see anything that goes on in your systems, whether that activity is an attack or it is normal a~ctivity.

**What are the technical specifications of your systemsenvironment?**

First, specify the technical attributes of your systems environment. Examples of information specified here would include network diagrams and maps specifying thenumber and locations of hosts; operating systems for each host; the number and types of network devices such as routers, bridges, and switches; number and types of terminal servers and dial-up connections; and descriptors of any network servers, including types, configurations, and application software and versions running on each. If you run an enterprise network management system, specify it here.

**What are the technical specifications of your current security protections?**

Once you have described the technical attributes of your systems environment, describe the security protections you already have in place. Specify numbers, types, and locations of network firewalls, identification and authentication servers, data and link encryptors, antivirus packages, access control products, specialized security hardware (such as crypto accelerator hardware for Web servers), Virtual Private Networks, and any other security mechanisms on your systems.

**What are the goals of yourenterprise?**

Some IDSs have been developed to accommodate the special needs of certain industries or market niches such as electronic commerce, health care, or financial markets. Define the functional goals of your enterprise (there can be several goals associated with a single organization) that are supported by your systems.

**How formal is the system environment and management culture in your organization?**

Organizational styles vary, depending on the function of the organization and its traditional culture. For instance, military or other organizations that deal with national security issues tend to operate with a high degree of formality, especially when contrasted with university or other academic environments. Some IDSs offer features that support enforcement of formal use policies, with configuration screens that accept formal expressions of policy, and extensive reporting capabilities that do detailed reporting of policyviolations.

**What are your Security Goals and Objectives?**

Once you've specified the technical landscape of your organization's systems as well as the existing security mechanisms, it's time to articulate the goals and objectives you wish to attain by using an IDS.

**Is the primary concern of your organization protecting from threats originating outside yourorganization?**

Perhaps the easiest way to specify security goals is by categorizing your organization's threat concerns. Identify the concerns that your organization has regarding threats that originate outside the organization.

**Is your organization concerned about insiderattack?**

Repeat the last step, this time addressing concerns about threats that originate from within your organization, encompassing not only the user who attacks the system from within (such as a shipping clerk who attempts to access and alter the payroll system) but also the authorized user who oversteps his privileges thereby violating organizational security policy or laws (a customer service agent who, driven by curiosity, accesses earnings and payroll records for public figures).

**Does your organization want to use the output of your IDS to determine new needs?**

System usage monitoring is sometimes provided as a generic system management tool to determine when s ystemassets require upgrading orreplacement. When such monitoringis performed by an IDS, the needs for upgrade can show up as anomalous levels of user activity.

**Does your organization want to use an IDS to maintain managerial control (non-security related) over networkusage?**

In some organizations, there are system use policies that target user behaviors that may be classified as personnel management rather than system security issues. These might include accessing Web sites that provide content of questionable taste or value (such as pornography) or using organizational systems to send e-mail or other messages for the purpose of harassing individuals. Some IDSs provide features that accommodate detecting such violations of management controls.

**What Is Your Existing Security Policy?**

At this time, you should review your existing organization security policy. This will serve as the template against which features of your IDS will be configured. As such, you may find you need to augment the policy, or else derive the following items from it.

**How is itstructured?**

It is helpful to articulate the goals outlined in the security policy in terms of the standard security goals (integrity, confidentiality, and availability) as well as more generic management goals (privacy, protection from liability, manageability).

**What are the general job descriptions of your systemusers?**

List the general job functions of system users (there are commonly several functions assigned to a single user) as well as the data and network accesses that each function requires.

**Does the policy include reasonable use policies or other management provisions?**

As mentioned above, many organizations have system use policies included as part of securitypolicies.

**Has your organization defined processes for dealing with specific policy violations?**

It is helpful to have a clear idea of what the organization wishes to do when the IDS detects that a policy has been violated. If the organization doesn't intend to react to such violations, it may not make sense to configure the IDS to detect them. If, on the other hand, the organization wishes to actively respond to such violations, the IDS's operational staff should be informed of the organization's response policy so that they can deal with alarms in an appropriate manner.

**Strengths of Intrusion Detection Systems**

Intrusion detection systems perform the following functions well:

- Monitoring and analysis of system events and userbehaviors
- Testing the security states of system configurations
- Baselining the security state of a system, then tracking any changes to thatbaseline
- Recognizing patterns of system events that correspond to knownattacks.
- Recognizing patterns of activity that statistically vary from normalactivity
- Managing operating system audit and logging mechanisms and the data they generate
- Alerting appropriate staff by appropriate means when attacks aredetected

- Measuring enforcement of security policies encoded in the analysisengine
- Providing default information securitypolicies
- Allowing non-security experts to perform important security monitoringfunctions

**Limitations of Intrusion Detection Systems**

Intrusion detection systems cannot perform the following functions:

- Compensating for weak or missing security mechanisms in the protection infrastructure. Such mechanisms include firewalls, identification and authentication, link encryption, access control mechanisms, and virus detection anderadication.
- Instantaneously detecting, reporting, and responding to an attack, when there is a heavy network or processingload
- Detecting newly published attacks or variants of existingattacks
- Effectively responding to attacks launched by sophisticatedattackers
- Automatically investigating attacks without humanintervention
- Resisting attacks that are intended to defeat or circumventthem
- Compensating for problems with the fidelity of informationsources
- Dealing effectively with switchednetworks

## 4.4 DEPLOYMENT AND IMPLEMENTATION OF AN IDS

**Q4. Write a short notes deployment and accers of ne/w on IDS**

**(a) Network base IDS**

**(b) Hotspot base IDS**

**(c) Application base IDS**

*Ans :*

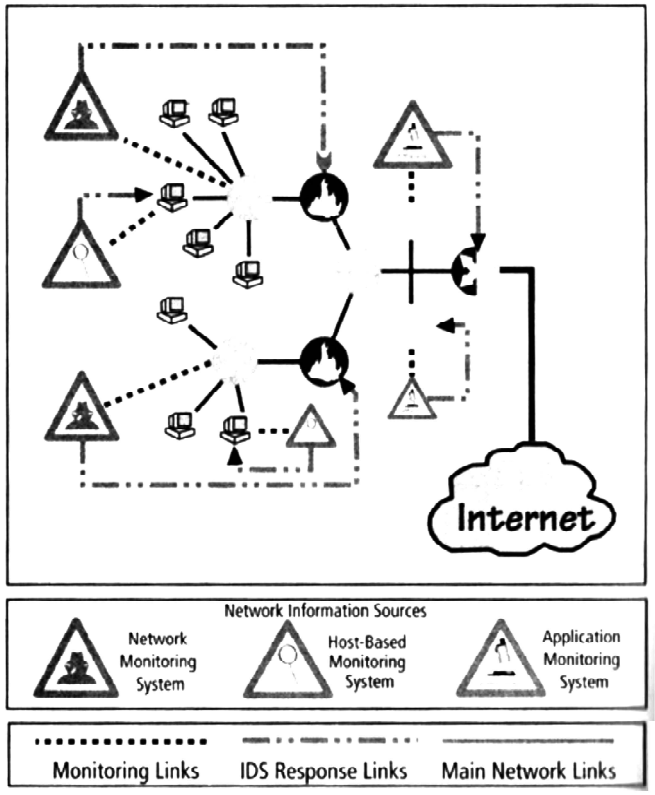
Deploying and implementing an IDS is not always a straight forward task. The strategy for deploying an IDS should consider a number of factors, the foremost being how the IDS will be managed and where it should be placed. These factors will determine the number of administrators needed to install, configure, and monitor the IDS, as well as the number of management workstations, the size of the storage needed for retention of the data generated by the systems, and the ability of the organization to detect and respond to remote threats.

**IDS Control Strategies**

An IDS can be implemented via one of three basic control strategies. A control strategy determines how an organization exerts influence and maintains the configuration of an IDS. It will also determine how the input and output of the IDS is to be managed. The three commonly utilized control strategies are centralized, partially distributed, and fully distributed. The IT industry has been exploring technologies and practices to enable the distribution of computer processing cycles and data storage for many years. These explorations have long considered the advantages and disadvantages of the centralized strategy versus those of strategies with varying degrees of distribution. In the early days of computing, all systems were fully centralized, resulting in a control strategy that provided high levels of security and control, as well as efficiencies in resource allocation and management. During the '80s and '90s, with the rapid growth in networking and computing capabilities, the IT industry's ideas about how to arrange computing systems swung to the other end of the pendulum-that is, the trend was to implement a fully distributed strategy. In the mid- '90s, however, the high costs of a fully distributed architecture became apparent, and the IT industry shifted toward a mixed strategy of partially distributed control. A strategy of partial

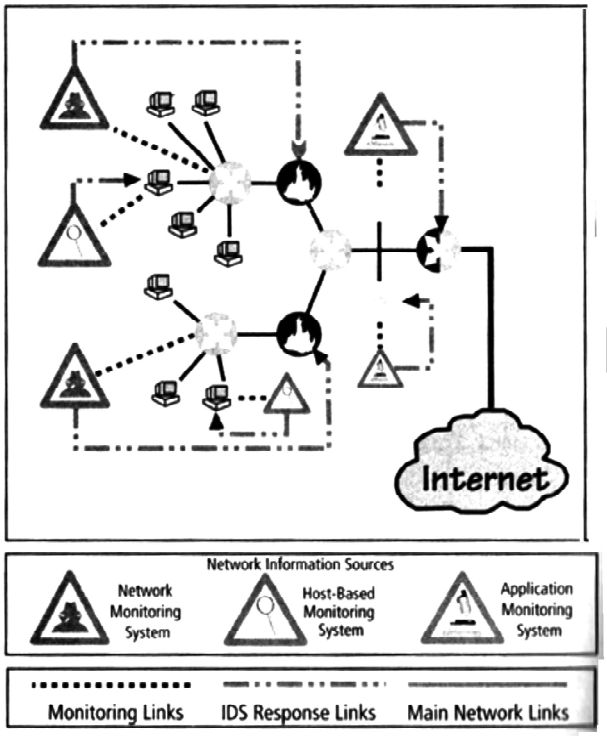
distribution, where some features and components are distributed and others are centrally controlled, has now emerged as the recognized recommended practice for IT systems in general and for IDS control systems in particular.

Centralized Control Strategy with a centralized IDS control strategy all IDS control functions are implemented and managed in a central location. This is indicated, in the figure with the large square symbol labeled "IDS Console." The IDS console includes the management software; which collects information from the remote sensors (appearing in the figure as triangular symbols), analyzes the systems or networks monitored, and makes the determination as to whether the current situation has deviated from the preconfigured baseline. All reporting features are also implemented and managed from this central location. The primary advantages of this strategy are related to cost and control. With" one central implementation, there is one management system, one place to go to monitor the status of the systems or networks, one location for reports, and one set of administrative management. This centralization of IDS management supports specialization in tasks, since all managers are either located near the IDS management console or can acquire an authenticated remote connection to it, and technicians are located near the remote sensors. This means that each person can focus specifically on the assigned task at hand. In addition, the central control group can evaluate the systems and networks as a whole, and since it can compare pieces of information from all sensors, the group is better positioned to recognize a large-scale attack.




Fully Distributed IDS Control[14]

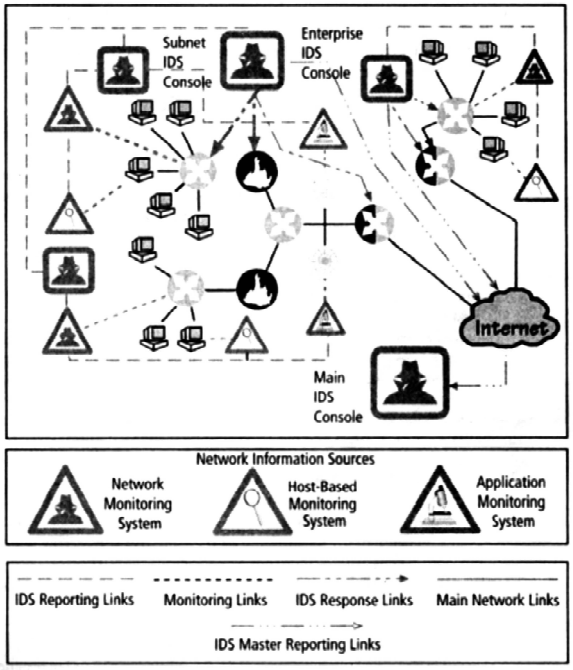
Fully Distributed Control Strategy a fully distributed IDS control strategyis the opposite of the centralized strategy. Note in the figure that all control functions (which appear as small square symbols enclosing a computer icon) are applied at the physical location of each IDS component. Each monitoring site uses its own paired sensors to perform its own control functions to achieve the necessary detection, reaction, and response functions. Thus, each sensor/agent is best configured to deal with its own environment. Since the IDSs do not have to wait for a response from a centralized control facility, their reaction to individual attacks is greatly speeded up.




Fully Distributed IDS Control[14]

**Partially Distributed Control Strategy.**Finally, a partially distributed IDS control strategy, as depicted, combines the best of the other two strategies. While the individual agents can still analyze and respond to local threats, their reporting to a hierarchical central facility enables the organization to detect widespread attacks. This blended approach to reporting is one of the more effective methods of detecting intelligent attackers, especially those who probe an organization through multiple points of entry, trying to scope out the systems' configurations and weaknesses, before they launch a concerted attack. The partially distributed control strategy also allows the organization to optimize for economy of scale in the implementationofkeymanagementsoftwareandpersonnel,especiallyinthereportingareas.

When the organization can create a pool of security managers to evaluate reports from multiple distributed IDS systems, it becomes better able to detect these distributed attacks before they become unmanageable.




Partially Distributed IDS Control[15]

## IDS Deployment Overview

Like the decision regarding control strategies, the decisions about where to locate the elements of the intrusion detection systems can be an art in itself. Given the highly technical skills required to implement and configure IDSs and the imperfection of the technology, great care must be made in the decisions about where to locate the components, both in their physical connection to the network and host devices and in how they will be logically connected to each other and the IDS administration team. Since IDSs are designed to detect, report, and even react to anomalous stimuli, placing IDSs in an area where such traffic is common can result in excessive reporting. Moreover, the administrators monitoring systems located in such areas can become desensitized to the high level of information flow and may fail to detect actual attacks in progress.

As an organization selects an IDS and prepares for implementation, planners must select a deployment strategy that is based on a careful analysis of the organization's information security requirements and that integrates with the organization's existing IT infrastructure but, at the same time, causes minimal impact. After all, the purpose of the IDS is to detect anomalous situations- not create them. One consideration for implementation is the skill level of the personnel required to install, configure, and maintain the systems.

An IDS is a complex system in that it involves numerous remote monitoring agents (on both individual systems and networks) that require proper configuration to gain the proper authentication and authorization. As the IDS is deployed, each component should be installed, configured, fine-tuned, tested, and monitored. A problem in any step of the deployment process may produce a range of problems-from a minor inconvenience to a network-wide disaster. Thus, both the individuals installing the IDS and the individuals using and managing the system require proper training.

NIDS and HIDS can be used in tandem to cover both the individual systems that connect to an organization's networks and the networks themselves. To do this, it is important for an organization to use a phased implementation strategy so as not to impact the entire organization all at once. A phased implementation strategy also allows security technicians to resolve the problems that do arise without compromising the very information security the IDS is installed to protect. In terms of sequencing the implementation, first the organization should implement the network-based IDS, as they are less problematic and easier to configure than their host -based counterparts. After the NIDSs are configured and running without issue, the HIDSs can be installed to protect the critical systems on the host server. Next, after both are considered operational, it would be advantageous to scan the network with a vulnerability scanner like Nmap or Nessus to determine if a) the scanners pick up anything new or unusual, and b) if the IDS can detect thescans.

**Deploying Network-Based IDSs**. As discussed above, the placement of the sensor agents is critical to the operation of all IDSs, but this is especially critical in the case of Network IDSs. NIST recommends four locations for NIDS sensors:

**Advantages:**

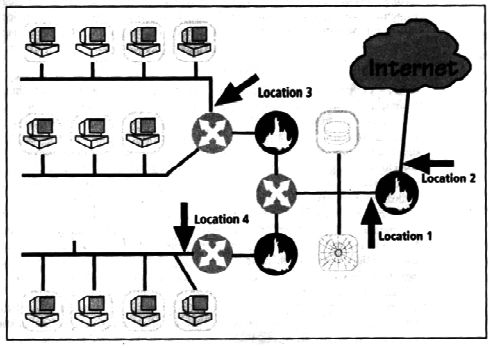
- IDS sees attacks that originate from the outside world and may penetrate the network's perimeterdefenses.
- IDS can identify problems with the network firewall policy orperformance.
- IDS see sattacks that might target the Webserveror fipserver, both of which commonly reside in this DMZ.

Even if the incoming attack is not detected, the IDS can sometimes recognize, in the outgoing traffic, patterns that suggest that the server has been compromised.

**Advantages:**

- IDS documents the number of attacks originating on the Internet that target thenetwork.
- IDS documents the types of attacks originating on the Internet that target thenetwork.
- IDS monitors a large amount of a network's traffic, thus increasing its chances of spottingattacks.
- IDS detects unauthorized activity by authorized users within the organization's security perimeter.
- IDS detects attacks targeting critical systems andresources.

Location allows organizations with limited resources to focus these resources on the network assets considered of greatest value.




Network IDS Sensor Locations[17]

**Deploying Host-Based IDSs**. The proper implementation of HIDSs can be a painstaking and time-consuming task, as each HIDS must be custom configured to its host systems. Deployment begins with implementing the most critical systems first This poses a dilemma for the deployment team, since the first systems to be implemented are mission-critical and any problems in the installation could be catastrophic to the organization. As such, it may be beneficial to practice an implementation on one or more test servers configured on a network segment that resembles the mission-critical systems. Practicing will help the installation team gain experience and also help determine if the installation might trigger any unusual events. Gaining an edge on the learning curve by training on non-production systems will benefit the overall deployment process by reducing the risk of unforeseencomplications.

Installation continues until either all systems are installed, or the organization reaches the planned degree of coverage it is willing to live with, with regard to the number of systems or percentage of

network traffic. Lastly, to provide ease of management, control, and reporting, each HIDS should , as discussed earlier, beconfigured to interact with a central management console.

Just as technicians can install the HIDS in off-line systems to develop expertise and identify potential problems, users and managers can gain expertise and understanding of the operation of the HIDS by using a test facility. This test facility could use the off-line systems configured by the technicians, but also be connected to the organization's backbone to allow the HIDS to process actual network traffic. This setup Will also enable technicians to create a baseline of normal traffic for the organization. During the system testing process, training scenarios can be developed that will enable users to recognize and respond to common attack situations. Finally, to ensure effective and efficient operation, the management team can establish policy for the operation and monitoring of theHIDS.

**Measuring the Effectiveness of IDSs**

IDSs are evaluated using two dominant metrics: first, administrators evaluate the number of attacks detected in a known collection of probes; second, the administrators examine the level of use, commonly measured in megabits per second of network traffic, at which the IDSs fail. An evaluation of an IDS might read something like this: at ]00Mb/s, the IDS was able to detect 97% of directed attacks. This is a dramatic change from the previous method used for assessing IDS effectiveness, which was based on the total number of signatures the system was currently running-a sort of "more is better" approach. Unfortunately, this evaluation method of assessment was flawed for several reasons. Not all IDSs use simple signature-based detection. Some systems, as discussed earlier, can use the almost infinite combination of network performance characteristics of statistical-anomaly-based detection to detect a potential attack. Also, some more sophisticated signature-based systems actually use fewer signatures/rules than older, simpler versions-which, in direct contrast to the signature-based assessment method, suggest that less may actually be more. The recognition that the size of the signature base is an insufficient measure of an IDS' effectiveness led to the development of stress test measurements for evaluating IDS performance. These only work, however, if the administrator has a collection of known negative and positive actions that can be proven to elicit a desired response. Since developing this collection can be tedious, most IDS vendors provide testing mechanisms that verify that their systems are performing as expected. Some of these testing processes will enable the administrator to:

- Record and retransmit packets from a real virus or wormscan
- Record and retransmit packets from a real virus or worm scan with incomplete TCP/IP session connections (missing SYNpackets)
- Conduct a real virus or worm scan against an invulnerablesystem

This last measure is important, since future IDSs will probably include much moredetailed information about the overall site configuration. According to experts in the field, "it may be necessary for the IDSs to be able to actively probe a potentially vulnerable machine, in order to either pre-load its configuration with correct information, or perform a retroactive assessment An IDS that performed some kind of actual system assessment would be a complete failure in today's generic testing labs, which focus on replaying attacks and scans against non existent machines.

With the rapid growth in technology, each new generation of IDSs will require new testing methodologies: However, the measured values that will continue to be of interest to IDS administrators and managers will, most certainly, include some assessment of how much traffic the IDS can handle, the numbers of false positives and false negatives it generates, and a measure of the IDSs ability to detect actual attacks. Vendors of IDSs systems could also include a report of the alarms sent and the relative accuracy of the system in correctly matching the alarm level to the true seriousness of the threat. Some planned metrics for IDSs may include the flexibility of signatures and detection policy customization.

IDS administrators may soon be able to purchase tools that test IDS effectiveness. Until these

tools are available from a neutral third party, the diagnostics from the IDS vendors will always be suspect. No matter how reliable the vendor, no vendor would provide a test their system wouldfail.

**One note of caution:** there may be a strong tendency among IDS administrators to use common vulnerability assessment tools, like Nmap or Nessus, to evaluate the capabilities of an IDS. While this may seem like a good idea, it will in fact not work as expected, because most IDS systems are equipped to recognize the differences between a locally implemented vulnerability assessment tool and a true attack.

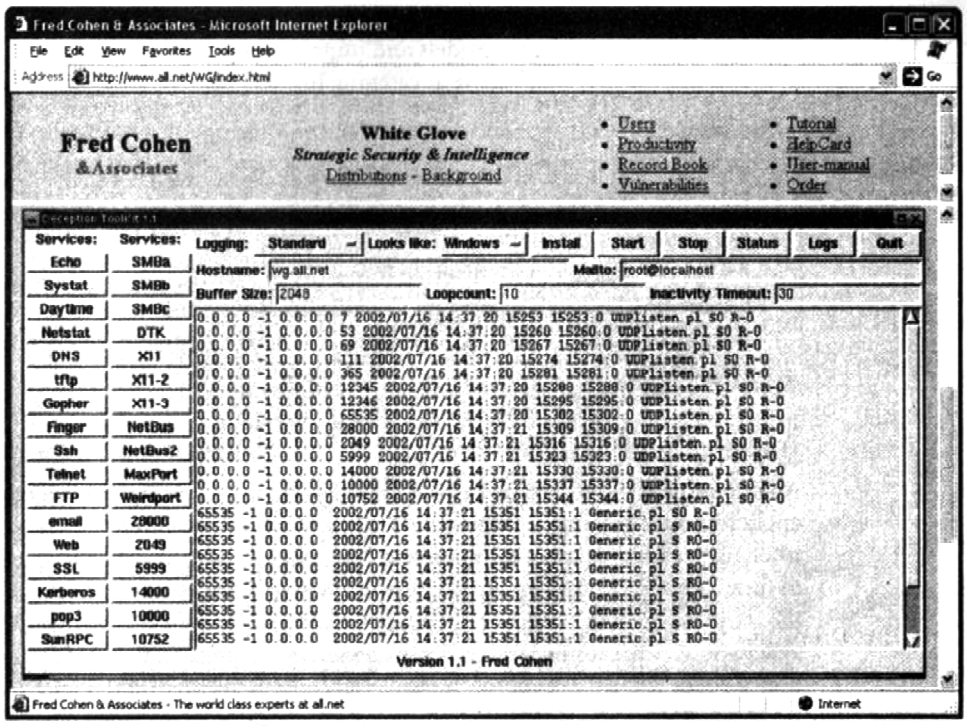
In order to perform a true assessment of the effectiveness of IDS systems, the test process should be as realistic as possible in its simulation of an actual event. This means coupling realistic traffic loads with realistic levels of attacks. One can not expect an IDS to respond to a few packet probes as if they represent a denial-of-service attack. In one reported example, a program was used to create a synthetic load of network traffic made up of many TCP sessions, with each session consisting of a SYN (or synchronization) packet, a series of data, and ACK (or acknowledgement) packets, but 110 FIN or connection termination packets. Of the several IDS systems tested, one of them crashed due to lack of resources while it waited for the sessions to be closed. Another IDS passed the test with flying colors because it did not perform state tracking on the connections. Neither of the tested IDS systems worked as expected, but the one that didn't perform state tracking was able to stay operational and was, therefore, given a better score on the test.

### Honey Pots, Honey Nets, and Padded Cell system

A class of powerful security tools that go beyond routine intrusion detection is known variously as honey pots, honey nets, or padded cell systems. To realize why these tools are not yet widely used, you must understand how these products differ from a traditional IDS. Honey pots are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves. Indeed, these systems are created for the sole purpose of deceiving potential attackers. In the industry, they are also known as decoys, lures, and fly-traps. When a collection of honey pots connects several honey pot systems on a subnet, it may be called a honey net. A honey pot system (or in the case of a honey net, an entire sub network) contains pseudo-services that emulate well-known services but is configured in ways that make it look vulnerable-that is, easily subject to attacks. This combination of attractants (i.e., attractive features such as the presence of both well-known services and vulnerabilities) is meant to lure potential attackers into committing an attack, and thereby revealing their existence-the idea being that once organizations have detected these attackers, they can better defend their networks against future attacks against real assets. In sum, honey pots are designedto:

- Divert an attacker from accessing criticalsy-stems
- Collect information about the attacker's activity
- Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps,respond.

Honey pot systems are filled with information that is designed to appear valuable (hence the name honey pots), but this information is fabricated and would not even be useful to a legitimate user of the system. Thus, any time a honey pot is accessed, this constitutes suspicious activity. Honey pots are instrumented with sensitive monitors and event loggers that detect these attempts to access the system and collect information about the potential attacker's activities. A screenshot from a simple IDS that specializes in honey pot techniques, called Deception Toolkit. This screenshot shows the configuration of the honey pot as it is waiting for an attack.




Deception Toolkit

Padded cells take a different approach. A **padded cell** is a honey poi that has been protected so that that it cannot be easily compromised. In other words, a padded cell is a hardened honey pot. In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDS. when the IDS detects attackers, it seamlessly transfers them to a special simulated environment where they can cause no harm-the nature of this host environment is what gives the approach its name, padded cell. As in honey pots, this environment (an befilledwith interesting data, some of which can be designed to convince an attacker that the attack is going according to plan. Like honeypots, padded cells are well-instrumented and offer unique opportunities for a would-be victim organization to monitor the actions of an attacker.

IDS researchers have used padded cell and honey pot systems since the late 1980s, but until recently no commercial versions of these products were available. It is important to seek guidance from legal counsel before deciding to use either of these systems in your operational environment, since using an attractant and then launching a back-hack or counterstrike might be construed as an illegal action and make the organization subject to a lawsuit or a criminal complaint.

The advantages and disadvantages of using the honey pot or padded cell approach are summarized below:

**Advantages:**

- Attackers can be diverted to targets that they cannotdamage.
- Administrators have time to decide how to respond to anattacker.
- Attacker's actions can be easily and more extensively monitored and the records can be used to refine threat models and improve systemprotections.

- Honey pots may be effective at catching insiders who are snooping around anetwork.

**Disadvantages:**

- The legal implications of using such devices are not welldefined.
- Honey pots and padded cells have not yet been shown to be generally useful security technologies.
- An expert attacker, once diverted into a decoy system, may become angry and launch a more hostile attack against an organization'ssystems.
- Administrators and security managers will need a high level of expertise to use these systems.

## 4.5 TRAP AND TRACESYSTEMS

**Q5. Explaing different techniques used to secure information using Trap & Trace system?**

*Ans :*

An extension of the attractant -based technologies in the preceding section, trap and trace applications are growing in popularity. These systems, often simply referred to as trap and trace, use a combination of techniques to detect an intrusion and then to trace incidents back to theirsources. The trap usually consists of a honey pot or padded cell and an alarm. While the intruders are distracted, or trapped, by what they perceive to be successful intrusions, the system notifies the administrator of their presence. The trace feature is an extension to the honey pot or padded cell approach. Similar in concept to caller ID, the trace is a process by which the organization attempts to determine the identity of someone discovered in unauthorized areas of the network or systems. If this individual turns out to be someone inside the organization, the administrators are completely within their power to track the individual down and turn them over to internal or external authorities. If the individual is outside the security perimeter of the organization, then numerous legal issues arise. One of the most popular professional trap and trace software suites is ManHunt, by Recourse Technologies. *It includes* a companion product, ManTrap, which is the honey pot application and thus presents a virtual network running from a single server. ManHunt is an intrusion detection system with the capability of initiating a track back function that can trace a detected intruder *as* far as the administrator wishes. Although administrators usually trace an intruder back to their organization's information security boundary, it is possible, with this technology, for them to coordinate with an ISP that has similar technology and thus hand off a trace to an upstream neighbor.

On the surface, trap and trace systems seem like an ideal solution. Security is no longer limited to defense. Now the security administrators can go on the offense. They can track down the perpetrators and turn them over to the appropriate authorities. Under the guise of justice, some less scrupulous administrators may even be tempted to back-hack, or hack into a hacker's system to find out as much as possible about the hacker. Vigilante justice would be a more appropriate term for these activities, which are in fact deemed unethical by most codes of professional conduct. In tracking the hacker, administrators may end up wandering through other organizations' systems, especially when the wily hacker may have used IP spoofing, compromised systems, or a myriad of other techniques to throw trackers off the trail. The result is that the administrator becomes a hacker himself, and therefore defeats the purpose of catching hackers.

There are more legal drawbacks to trap and trace. The trap portion frequently involves the use of honey pots or honey nets. When using *honey* pots and honey nets, administrators should be careful not to cross the line between enticement and entrapment. Enticement is the process of attracting attention to a system by placing tantalizing bits of information in key locations. Entrapment is the action of luring an individual into committing a crime to get a conviction. Enticement is legal and ethical, where as entrapment is not. It is difficult to gauge the effect such a system can have on the average user, especially if the individual has been nudged into looking at the information. Administrators should also be wary of the wasp trap syndrome. In this syndrome, a concerned homeowner installs a wasp trap in his back yard to trap the few insects he

sees flying about. Because these traps use scented bait, however, they wind up attracting far more wasps than were originally present. Security administrators should keep the wasp trap syndrome in mind before implementing honey pots, honey nets, padded cells, or trap and trace systems.

**Active Intrusion Prevention**

Some organizations would like to do more than simply wait for the next attack and implement active countermeasures to stop attacks. One tool that provides active intrusion prevention is known as LaBrea(http://www.labreatechnologies.com). LaBrea works by taking up the unused IP address space within a network. When LaBrea notes an ARP request, it checks to see if the IP address requested is actually valid on the network. If the address is not currently being used by a real computer or network device, LaBrea will pretend to be a computer at that IP address and allow the attacker to complete the TCP/IP connection request, known as the three-way handshake. Once the handshake is complete, LaBrea will change the TCP sliding window size down to a low number to hold the TCP connection from the attacker open for many hours, days, or even months. Holding the connection open but inactive greatly slows down network-based worms and other attacks. It allows the LaBreasystem time then to notify the system and network administrators about the anomalous behavior on the network.

## 4.6 Scanning and Analysis Tools

**Q6. What are the purposes of scanning and analysis tools? Who will be using these tools?**

*Ans :*

In order to secure a network, it is imperative that someone in the organization knows exactly where the network needs securing. This may sound like a simple and intuitive statement; however, many companies skip this step. They install a simple perimeter firewall, and then, lulled into a sense of security by this single layer of defense, they rest on their laurels. To trulyass ess the risk with in a computing environment, one must deploy technical controlsusing a strategy of defense in depth. A strategy based on the concept of defense in depth is likely to include intrusion detection systems (IDS), active vulnerability scanners, passive vulnerability scanners, automated log analyzers, and protocol analyzers (commonly referred to as sniffers). As you've learned, the first item in this list, the IDS, helps to secure networks by detecting intrusions; the remaining items in the list also help secure networks, but they do this by helping administrators identify where the network needs securing. More specifically, scanner and analysis tools can find vulnerabilities in systems, holes in security components, and unsecured aspects of the network.

Although some information security experts may not perceive.them as defensive tools, scanners, sniffers, and other such vulnerability analysis tools can be invaluable to security administrators because they enable administrators to see what the attacker sees. Some of these tools are extremely complex and others are rather simple. The tools can also range from being expensive commercial products to those that are freely available at no cost. Many of the best scanning and analysis tools .are those that the attacker community has developed, and are available free on the Web. Good administrators should have several hacking Web sites' bookmarked and should try to keep up with chat room discussions on new vulnerabilities, recent conquests, and favorite assault techniques. There is nothing wrong with a security administrator using the tools that potential attackers use in order to examine his or her defenses and find areas that require additional attention. In the military, there is a long and distinguished history of generals inspecting the troops under their command before battle, walking down the line checking out the equipment and mental preparedness of each soldier. In a similar way, the security administrator can use vulnerability analysis tools to inspect the units (host computers and network devices) under his or her command. A word of caution, though, should be heeded: many of these scanning and analysis tools have distinct signatures, and Some Internet service providers (ISPs) scan for these signatures. If the ISP discovers someone using hacker tools, it can pull that person's access privileges. As such, it is probably best for administrators first to establish a working relationship with their ISPs and notify the ISP of theirplans.

Scanning tools are, as mentioned earlier, typically used as part of an attack protocol to collect information that an attacker would need to launch

a successful attack. The attack protocol is a series of steps or processes used by an attacker, in a logical sequence, to launch an attackagainst a target system or network. One of the preparatory parts of the attack protocol is the collection of publicly available information about a potential target, a process known as footprinting.

**Footprinting**is the organized research of the Internet addresses owned or controlled by a target organization. The attacker uses public Internet data sources to perform keyword searches to identify the network addresses of the organization. This research is augmented by browsing the organization's Web pages. Web pages usually contain quantities of information about internal systems, individuals developing Web pages, and other tidbit~, which can be used for social engineering attacks. The View Source option on most popular Web browsers allows the user to see the source code behind the graphics. A number of details in the source code of the Web page can provide clues to potential attackers and give them insight into the configuration of an internal network, such as the locations and directories for Common Gateway Interface (CGI) script bins and the names or possibly addresses of computers and servers. In addition, public business Web sites (such as Forbes, or Yahoo Business) will often reveal information about company structure, commonly used company names, and other information that attackers find useful. Further more, common search engines will allow attackers to query for any site that links to their proposed target. By doing a little bit of initial Internet research into a company, an attacker can often find additional Internet locations that are not commonly associated with the company-that is, Business to Business (B2B) partners and subsidiaries. Armed with this information, the attacker can find the "weakest link" into the target network.

For an example, consider Company X, which has a large datacenter located in Atlanta. The data center has been secured, and thus it will be very hard for an attacker to break into the datacenter via the Internet. However, the attacker has run a "link" query on the search engine www.altavista.com and found a small Web server that links to Company X's main Web server. After further investigation, the attacker learns that the small Web server was set up by an administrator at a remote facility and that the remote facility has, via its own leased lines, an unrestricted internal link into Company X's corporate datacenter. The attacker can now attack the weaker site at the remote facility and use this compromised network-which is an internal network-to attack the true target. While it may seem trite or cliche, the phrase a chain is only as strong as its weak estlink is very relevant to network and computer security. If acompany has a trusted network connection in place with 15 business partners, even one weak business partner can compromise all 16 networks.To assist in the footprint intelligence collection process, another type of scanner can be used. This is an enhanced Web scanner that, among other things, can scan entire Web sites for valuable pieces of information, such as server names and e-mail addresses. Sam Spade can also do a host of other scans and probes, such as sending multiple ICMP information requests (Pings), attempting to retrieve multiple and cross-zoned DNS queries, and performing network analysis queries (known, from the commonly used UNIX command for performing the analysis, as traceroutes). All of these are powerful diagnostic and hacking activities. Sam Spade is not, however, considered to be hackerware (or hacker-oriented software), but rather it is a utility that happens to be useful to network administrators and miscreantsa like.For Linux or BSD systems, there is a tool called "wget" that allows a remote individual to "mirror" entire Web sites. With this tool, attackers can copy an entire Web site and then go through the source HTML, JavaScript, and Web-based forms at their leisure, collecting and collating all of the data from the source code that will be useful to them for their attack.


Sam Spade

The next phase of the attack protocol is a second intelligence or data-gathering process called finger printing. This is a systematic survey of all of the target organization's Internet addresses (which were collected during the footprinting phase described above); the survey is conducted to ascertain the network services offered by the hosts in that range. By using the tools discussed in the next section, finger printing reveals useful information about the internal structure and operational nature of the target system or network for the anticipated attack. Since these tools were created to find vulnerabilities in systems and networks quickly and with a minimum of effort, they are valuable for the network defender since they can quickly pinpoint the parts of the systems or network that need a prompt repair to close the vulnerability.

### Port Scanners

Port scanning utilities (or port scanners) are tools used by both attackers and defenders to identify (or fingerprint) the computers that are active on a network, as well as the ports and services active on those computers. The functions and roles the machines are fulfilling, and other useful information. These tools can scan for specific types of computers, protocols, or resources, or their scans can be generic. It is helpful to understand the environment that exists in the network *you* are using. so that you can use the tool most suited to the data collection task athand.

For instance, if you are trying to identify a Windows computer in a typical network, a built-in feature of the operating system, may be able to get the answer you need very quickly, without requiring the

installation of a scanner. This tool will not work on other types of networks, however, so you must know your tools in order to make the best use of the features of each.

The more specific the scanner is, the better it can give attackers and defenders information that is detailed and will be useful later. However, it is also recommended that you keep a generic, broad-based scanner in your toolbox as well. This helps to locate and identify rogue nodes on the network that administrators may be unaware of. Probably the most popular port scanner is Nmap, which runs on both Unix and Windows systems.

A port is a network channel or connection point in a data communications system. Within the TCP/IP networking protocol, TCP and User Datagram Protocol (UDP) port numbers differentiate the multiple communication channels that are used to connect to the network services being offered on the same network device. Each application within TCP/IP has a unique port number assigned. Some have default ports but can also use other ports. Some of the well-known port numbers are presented. In all, there are 65,536 port numbers in use for TCP and another 65,536 port numbers for UDP. Services using the TCP/IP protocol can run on any port; however, the services with reserved ports generally run on ports 1-1023. Port 0 is not used. Ports greater than 1023 are typically referred to as ephemeral ports and may be randomly allocated to server and client processes.

Why secure open ports? Simply put, an open port can be used by an attacker to send commands to a computer, potentially gain access to a server, and possibly exert control over a networking device. The general rule of thumb is to remove from service or secure any port not absolutely necessary to conducting business. For example, if a business doesn't host Web services. there may be no need for port 80 to be available on its servers.



**Commonly Used Port Numbers**

| TCP Port Numbers | TCP Service |
|---|---|
| 20 and 21 | File Transfer Protocol (FTP) |
| 22 | Secure Shell (SSH) |
| 23 | Telnet |
| 25 | Simple Mail Transfer Protocol (SMTP) |
| 53 | Domain Name Services (DNS) |
| 67 and 68 | Dynamic Host Configuration Protocol (DHCP) |
| 80 | Hypertext Transfer Protocol (HTTP) |
| 110 | Post Office Protocol (POP3) |
| 161 | Simple Network Management Protocol (SNMP) |
| 194 | IRC chat port (used for device sharing) |
| 443 | HTTP over SSL |
| 8080 | Used for proxy services |

Firewall Analysis Tools

## 4.7 FIREWALL ANALYSIS TOOLS

**Q7. What is the purpose of firewall analysis tools? Why?**

*Ans :*

Understanding exactly where an organizati-on's firewall is located and what the existing rule sets on the firewall do are very important steps for any security administrator. There are several tools that automate

the remote discovery of firewall rules and assist the administrator (or attacker) in analyzing the rules to determine exactly what they allow and what they reject.

The Nmap tool mentioned earlier has some advanced options that are useful for firewall analysis. The Nmap option called *Idle scanning* (which is run with the -I switch) will allow the Nmap user to bounce your scan across firewall by using one of the IDLE DMZ hosts as the initiator of the scan. More specifically, as most operating systems do not use truly random II' packet identification numbers (IP IDs), if there is more than one host in the DMZ and one host uses non-random IP IDs, then the attacker can query the server (server X) and obtain the currently used IP ID as well as the known algorithm for incrementing the IP IDs. The attacker can then spoof a packet that is allegedly & 001 server X and destined I or an internal II' address behind the firewall. If the port is open on the internal machine, the internal machine will replytoserver X with a SYN-ACK packet, which will force server X to respond with a TCI' RESET packet. In responding with the TCP RESET, server X increments its II' ID number. The attacker can now query server X a second time to see if the II' ID has incremented. If it has, the attacker knows that the internal machine is alive and that the internal machine has the queried service port open. In a nutshell, running the Nmap Idle scan allows an attacker to scan an internal network as if he or she were physically located on a trusted machine inside the DMZ.

Another tool that can be used to analyze firewalls is Firewalk. Written by noted author and network security expert Mike Schiffman, Firewalk uses incrementing Time-To-Live (TTL) packets to determine the path into a network as well as the default firewall policy. Running Firewalk against a target machine will reveal where routers and firewalls are filtering traffic to the target host. More information on Firewalk can be obtained from http://www.packetfactory.net/.

A final firewall analysis tool worth mentioning is HI'ING, which is a modified Ping client. It supports multiple protocols and has a command-line means of specifying nearly any of the Ping parameter,. For instance, you can use HPING with modified TTL values to determine the infrastructure of a DMZ. You can use HPING with specific ICMP flags in order to bypass poorly configured firewalls (i.e., firewalls that allow all ICMP traffic to pass through) and find internal systems. HPING can be found at http://www.hping.org/.

Incidentally, administrators who fed wary of using the same tools that attackers use should remember two important points: regardless of the nature of the tool that is used to validate or analyze a firewall's configuration, it is the intent of the user that will dictate how the information gathered will be used; in order to defend a computer or network well, it is necessary to understand the ways it can be attacked. Thus, a tool that can help close up an open or poorly configured firewall will help the network defender minimize the risk fromattack.

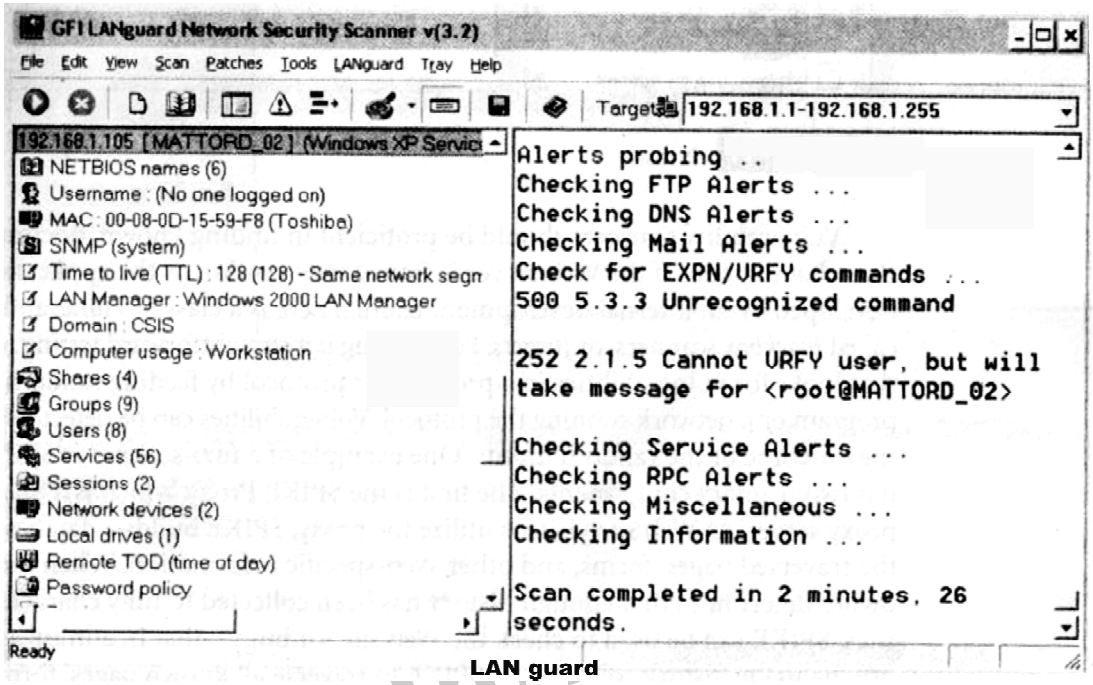
### Operating System Detection Tools

Detecting a target computer's operating system is, very valuable to an attacker, because once the as is known, all of the vulnerabilities to which it is susceptible can easily be determined. There are many tools that use networking protocols to determine a remote computer's as. One specific tool worth mentioning is XProbe, which uses ICMP to determine the remote OS. This tool can be found at http://wMi..sys-stcurity.cor/1/lrtmllprojectslX.html. When it's run, XProbe sends a lot ofdifferent ICMP queries against the target host. As reply packets are received, XProbe matches these responses from the target's TCP/IP stack with its own internal database of known responses. As most ass have a unique way of responding to ICMP requests, Xprobe is very reliable in finding matches and thus detecting the operating systems of remote computers. System and network administrators should take note of this, and plan to restrict the use of ICMP through their organization's firewalls and, when possible, within its internalnetworks.

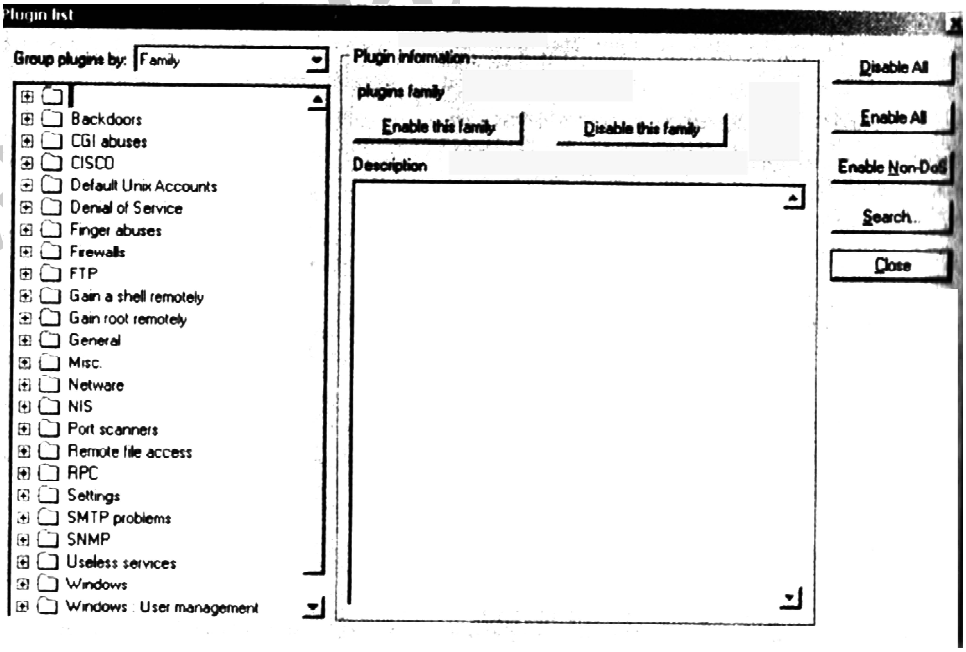
### Vulnerability Scanners

**Active vulnerability scanners** scan networks for highly detailed information. An *active* scanner is one that initiates traffic on the network in order to determine security holes. As a class, this type of scanner identities exposed usernames and groups, shows open network shares, and exposes configuration problems and other vulnerabilities in servers. An example of a vulnerability scanner is

GFI LAN guard Network Security Scanner (NSS), which is available as & freeware for non-commercial use. Another example of a vulnerability scanner is Nessus, which is a professional & freeware utility that uses IP packets to determine the hosts available on the network, the services (ports) they are offering, the operating system and as version they are running, the type of packet filters and firewalls in use, and dozens of other characteristics of the network.




**LAN guard**



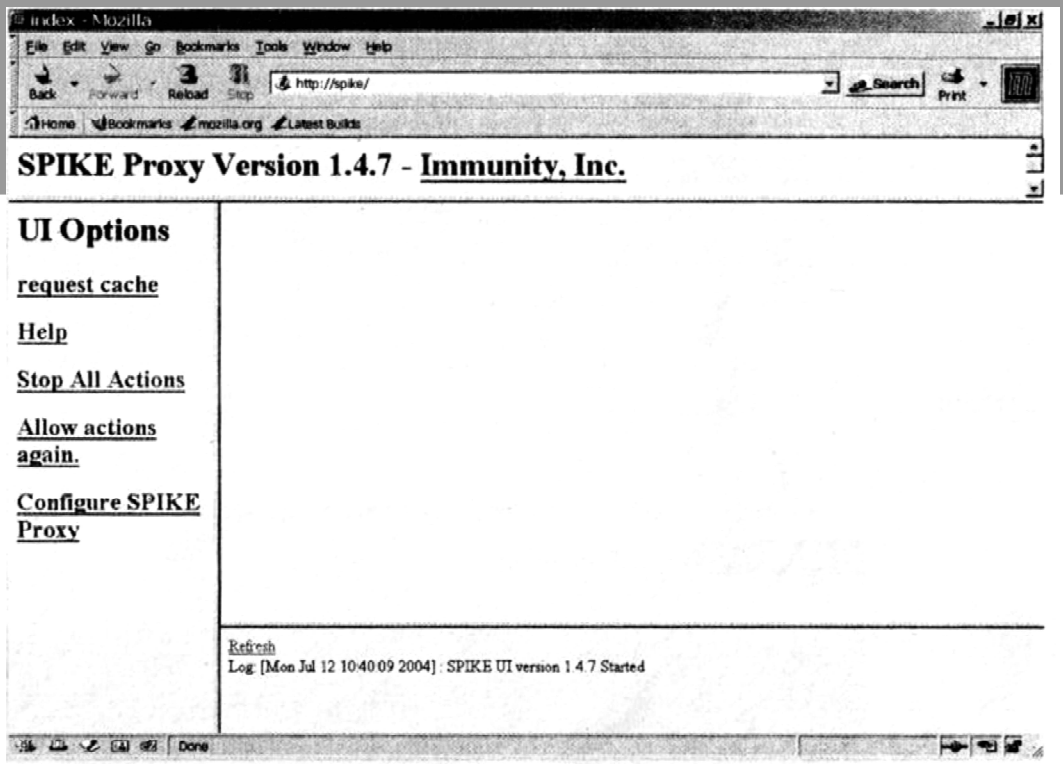

**Nessus**

Vulnerability scanners should be proficient in finding known, documented holes. But what happens if the Web server is from a new vendor, or the application was developed by an internal development team? There is a class of vulnerability scanners called *blackbox*scanners, or fuzzers. Fuzz testing is a

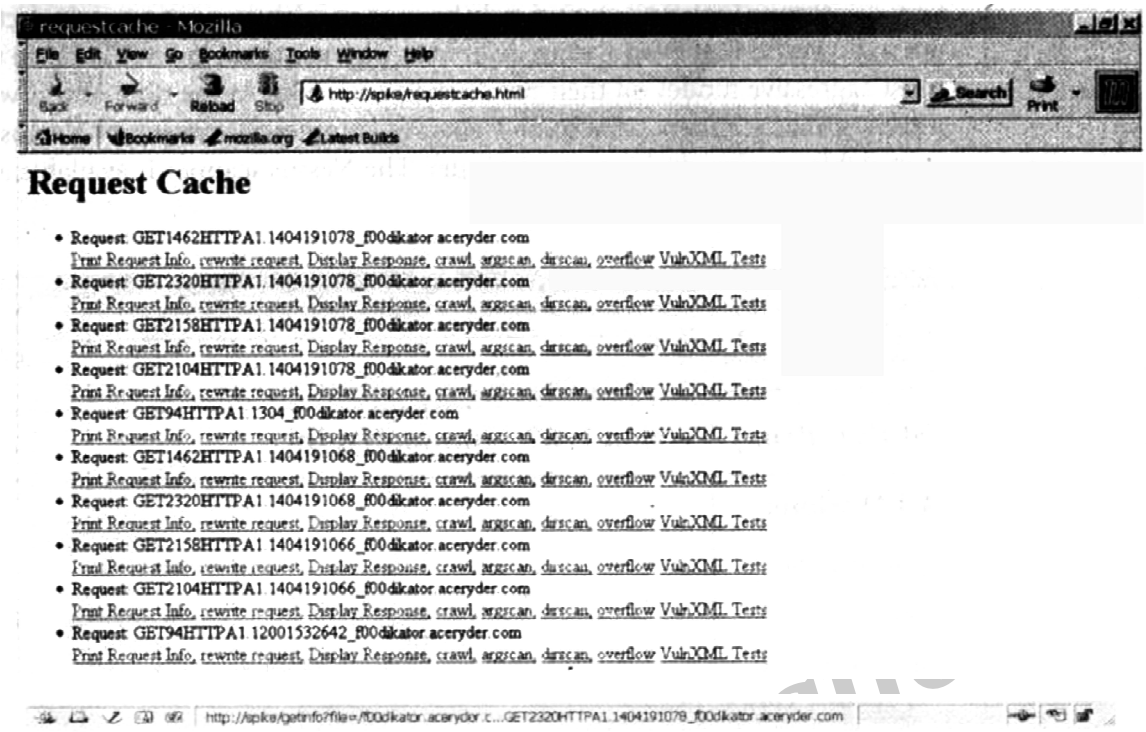
straightforward testing technique that looks for vulnerabilities in a program or protocol by feeding random input to the program or a network running the protocol. Vulnerabilities can be detected by measuring the outcome of the random inputs. One example of fuzz scanner is SPIKE, which has two primary components. The first is the SPIKE Proxy, which is a full-blown proxy server. As Website visitors utilize the proxy, SPIKE builds a database of each of the traversed pages, forms, and web-specific information, When the web site owner determines that enough history has been collected to fully characterize the web sites, SPIKE can be used to check the web site for bugs- that is, administrators can use the usage history collected by SPIKE to traverse all known pages, forms, active programs (e.g., asp, cgi-bin),etc., and can test the system by attempting overflows, SQL injection, cross-site scripting, and many other classes of Webattacks.

SPIKE also has a core functionality to fuzz any protocol that utilizes TCP/IP. By sniffing a session and building a SPIKE script, or building a full-blown C program using the SPIKE API, a user can stimulate and "fuzz" nearly any protocol. The spike PROXY configuration screen.A sample SPIKE script being prepared to fuzz the ISAKAMP protocol (which is used by VPNs).

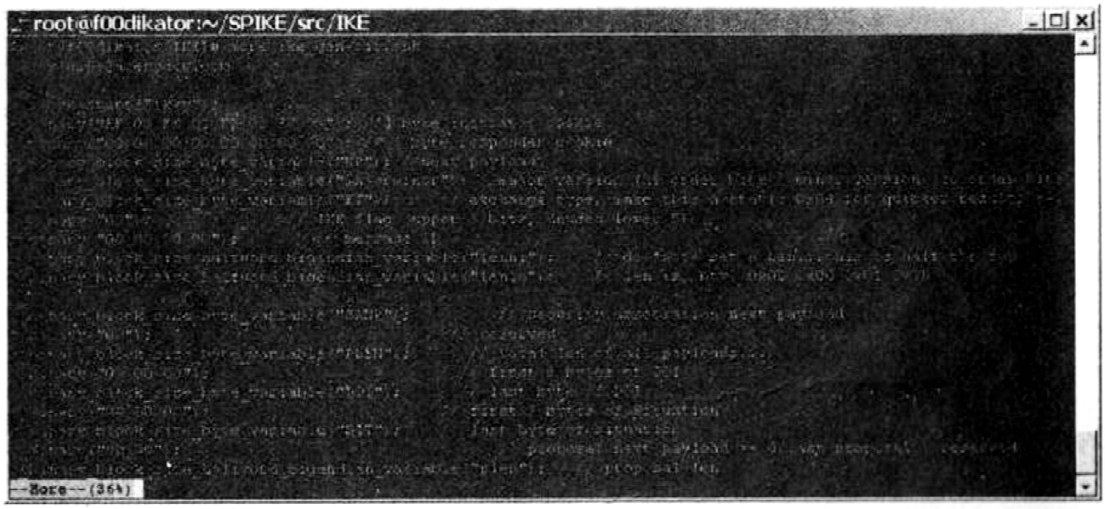
Similar in function, the previously mentioned scanner has a class of attacks called DESTRUCTIVE. If enabled, Nessus will attempt common overflow techniques against a target host. Fuzzers or blackbox scanners and Nesses in destructive mode can be every dangerous tool and should only be used in a lab environment. In fact, these tools are so powerful that even system defenders who use them are not likely to use them in the most aggressive modes on their production networks. At the time of this writing, the most popular scanners seem to be Nessus(a commercial version of Nessus for windows is available), retina, and Internet scanner. The Nessus scanner is available at no cost: the other two require a license fee.




SPIKE Proxy



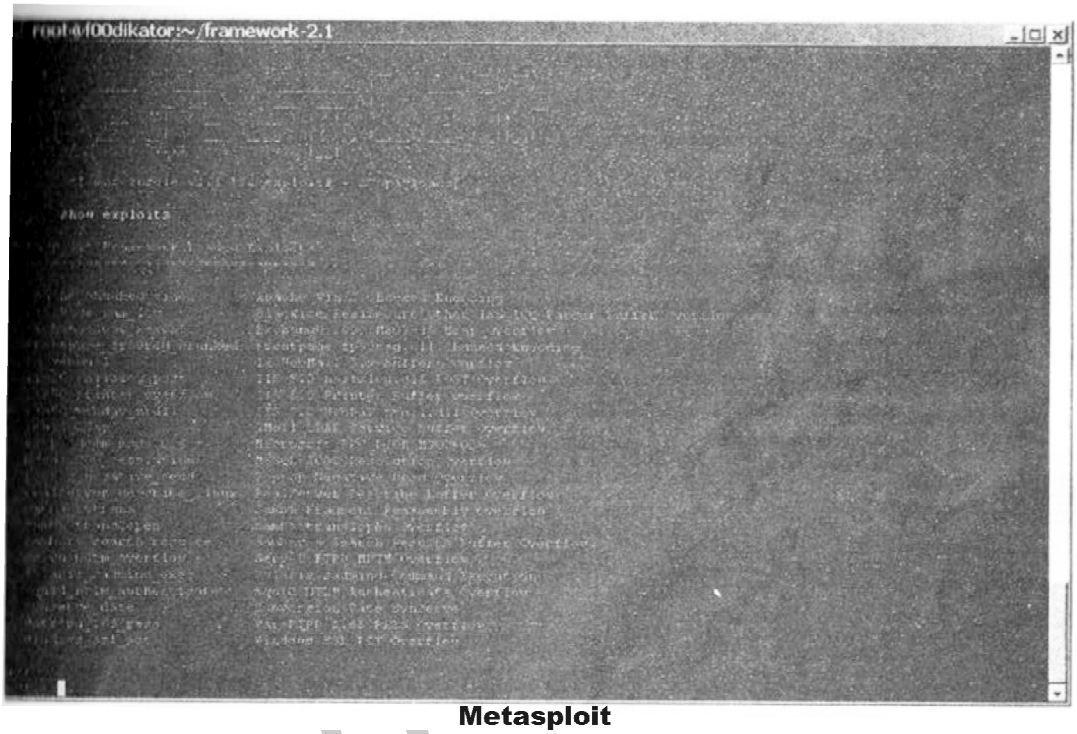

SPIKE In Action



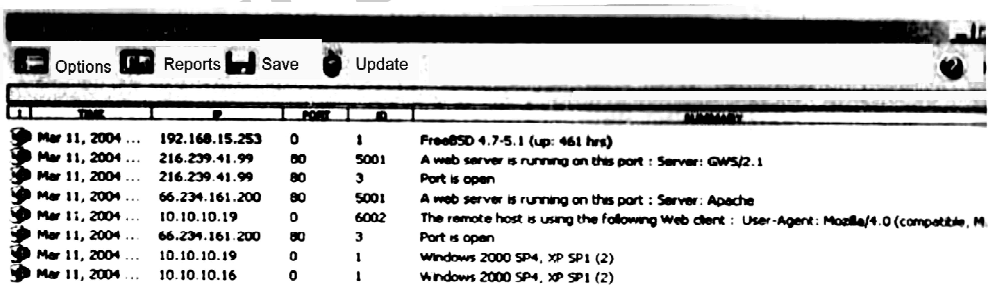

SPIKE vs. IKE

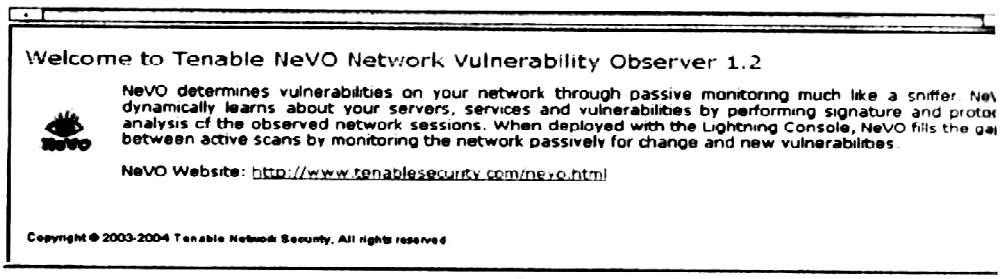
Often times, some members of an organization will require proof that a system is actuallyvulnerable to c certain attack. They may require such proof in order to avoid having system administrators attempt to repair system that are not in fact broken, or because they have not yet builtasatisfactoryrelationshipwiththevulnerabilityassessmentteam.Intheseinstances,thereexists a class of scanners that will actually exploit the remote machine and allow the vulnerability analyst (sometimes called penetration tester to create an account, modify a web page, or view data. These tools can be very dangerous and should only be used when absolutely necessary. Three tools that can perform this action are core Impact, Immunity's CANVAS, and the MetasploitFramework.

Of these three tools, only the Metasploit Framework is available without a license fee.The Metasploit Framework is a collection of exploits coupled with an interface that allows the penetration tester to automate the custom exploitation of vulnerable systems. So, for instance, if you wished to exploit a Microsoft Exchange server and run a single command (perhaps add the user "security" into the administrators group), the tool would allow you to customize the overflow in this manner.




**Metasploit**




**NeVO**

provides World Wide Web addresses for the products mentioned in the vulnerability scanners section.

**Vulnerability Scanner Products and Web Pages**

| Product | Web Page |
|---|---|
| Nessus | *http://www.nessus.org* |
| Nessus for Windows | *http://www.tenablesecurity.com* |
| GFI LANguard Network Security Scanner | *http://www.gfi.com/languard* |
| SPIKE - SPIKEproxy | *http://www.immunitysec.com* |
| Retina | *http://www.eeye.com* |
| Internet Scanner | *http://www.iss.net* |
| Core Impact | *http://www.coresecurity.com/home/home.php* |
| CANVAS | *http://www.immunitysec.com/CANVAS* |
| Metasploit Framework | *http://metasploit.com* |

A Passive vulnerability scanner is one that listens in on the network and determines vulnerable versions of both server and client software. At the time of this writing, there are two primary vendors offering this type of scanning solution: Tenable Network Security with its NeVO product and Source fire with its RNA product. Passive scanners are advantageous in that they do not require vulnerability analysts to get approval prior for testing. These tools simply monitor the network connections to and from a server to gain a list of vulnerable applications. Furthermore, passive vulnerability scanners have the ability to find client-side Vulnerabilities that are typically not found in active scanners. For instance, an active scanner operating without DOMAIN Admin rights would be unable to determine the version of Internet Explorer running on a desktop machine, whereas a passive scanner will be able to make that determination by observing the traffic to and from the client.

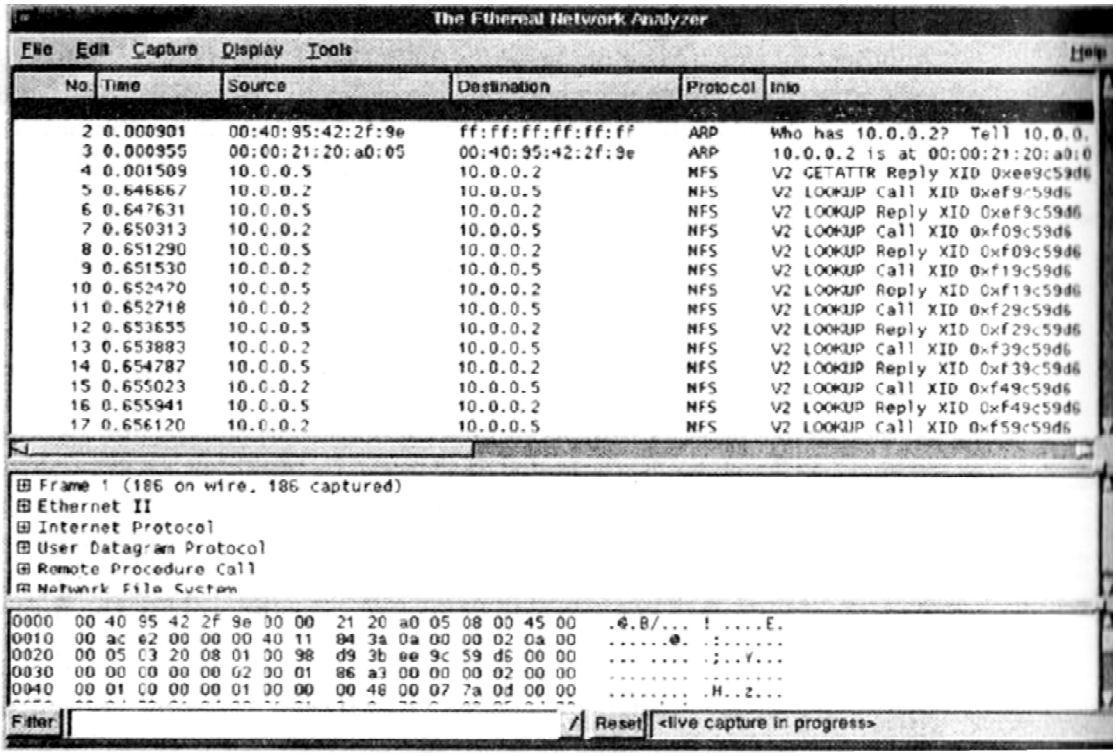
### Packet Sniffers

Another tool worth mentioning here is the packet sniffer. A packet sniffer (sometimes called a network protocol analyzer) is a network tool that collects copies of packets from the network and analyzes them. It can provide a network administrator with valuable information for diagnosing and resolving networking issues. In the wrong hands, however, sniffer can be used to eavesdrop on network traffic. There are both commercial and open-source sniffers- more specifically, sniffer is a commercial product, and snort is open-source software. An excellent free, client- based network protocol analyzer is Ethereal (www.ethereal.com). Ethereal allows the administrator to examine data from both live network traffic and captured traffic. Ethereal has several features, including a language filter and TCP session reconstruction utility.

A sample screen from Ethereal. Typically, to use these types of programs most effectively, the user must be connected to a network from a central location. Simply tapping into an Internet connection floods with you more data than can be readily processed, and technically constitutes a violation of the wire tapping act. To use a packet snifferle gally, the administrat or must: 1) beona network that organization owns, 2) be under direct authorization of the owners of the network, and 3) have knowledge and consent of the content creators. If all three conditions are met, the administrator can selectively collect and analyze

packets to identify and diagnose problems on the network. Conditions one and two are self-explanatory. The third, consent, is usually handled by having all system users sign a release when they are issued a user ID and passwords. Incidentally, these three items are the same requirements for employee monitoring in general, and packet sniffing should be constructed as a form of employeemonitoring.

Many administrators feel that they are safe from sniffer attacks when their computing environment is primarily a switched network environment. This couldn't be farther from the truth. There are a number of open-source sniffers that support alternate networking approaches that can, in turn, enable packet sniffing in a switched network environment. Two of these alternate networking approaches are ARP-Spoofing and session hijacking (which uses tools like ettercap). To secure data in transit across any network, organizations must be encryption to be assured of content privacy.

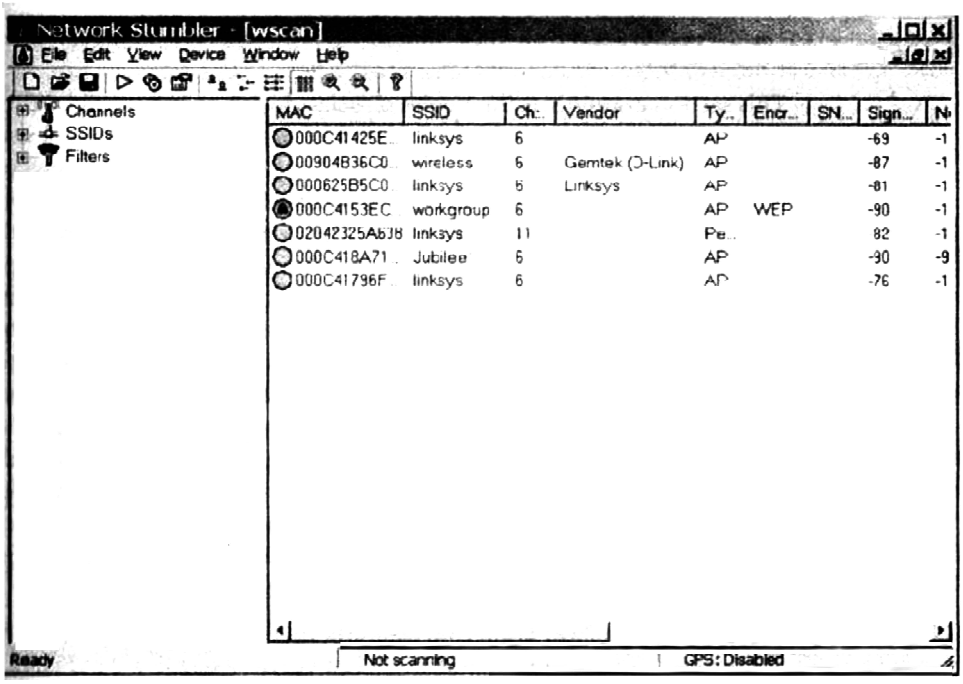



**Ethereal**

### Wireless Security Tools

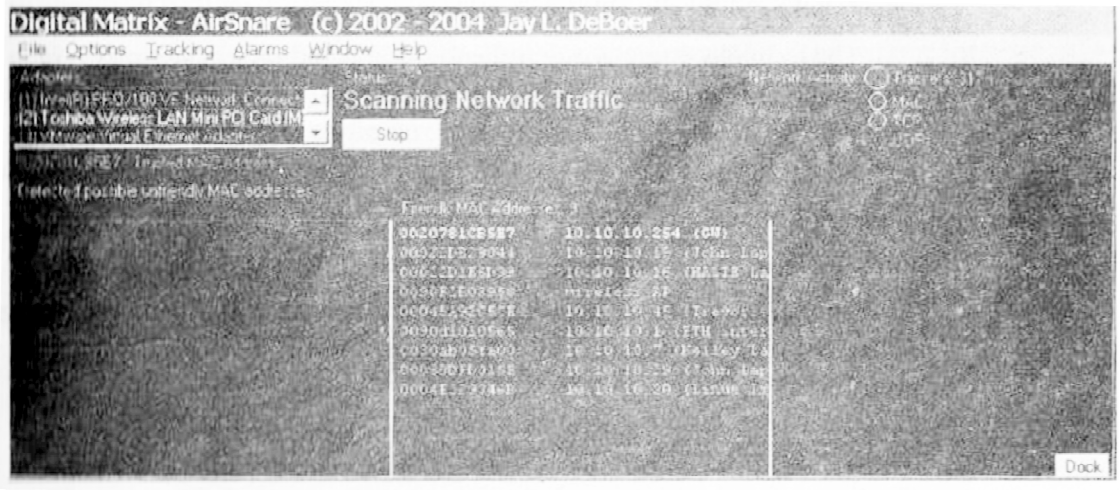
802.11 wireless networks have sprung up as subnets on nearly all large networks. A wireless connection, while convenient, has many potential security holes. An organization that spends all of its time securing the wired network and leaves wireless networks to operate in any manner is opening itself up for a security breach. As a security professional, you must access the risk of wireless networks A Wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and asses the level of privacy or confidentiality afford on the wireless network. There is a suite of tools from dachb0dens labs *(http:// www. Dachb0den.com/bsd- airtools.html*) called bsd-airtools that automates all of the items noted above. The tools included within the bsd-airtools toolset are an access point detection tool, a sniffer, and a tool called dstumbler to crack Wired Equivalent Protocol (WEP) encryption keys. A windows version of

the dstumbler tool called Netstumbler is also offered as freeware and can be found athttp:// www.Netstumbler.org. NetStumbler being run from a Windows XP machine. Another wireless tool worth mentioning is Airsnare. Airsnare is a free tool that can be run on a low-end wireless workstation. Airsnare monitors the airwaves for any new devices or Access Points. When it finds one Airsnarewill sound an alarm alerting the administrators that a new, potentially dangerous, wireless apparatus is attempting access on a closed wireless network.




**NetStumbler**

The tools discusseds of arhelpthe attac kerand the defenderpreparethe mselvestocomplete th e next steps in the attack protocol: attack, compromise, andexploit. These steps are beyond the scope of this text, for they are usually covered in more advanced classes on computer and network attack and defense.




**Air snare**

## 4.8 Access Control Devices

**Q8. What is access control? What are access control devices?**

*Ans :*

This section examines technologies associated with access control. When a prospective user, referred to in the area of access as a supplicant, seeks to use a protected system, logically access a protected service, or physically enter a protected space, he or she must engage in authentication and authorization activities to establish his or her identify and verify that he or she has permission to complete the requested activity. A successful access control systemincludesa number of components, depending on the system's needs for authentication and authorization. Occasionally a system will have a need for strong authentication when verifying supplicant's identity. Strong authentication requires at least two of the forms of authentication listed below to authenticate the supplicant's identity. Routine authentication has traditionally made use of only one form; and in many cases, this happens to be of the "What a supplicant knows" variety. This is why many systems familiar to us require a user ID and password (both examples of something known to the user) for authentication. When a second factor is required to verify the supplicant's identify. This is frequently a physical device, i.e., something the supplicant has, such as an ATM card or smart card. In terms of access control, there are four general forms of authentication to consider:

- **What a supplicant knows:** for example, user IDs andpassphrases
- **What a supplicant has:** often tokens and smartcards
- **Who a supplicant is :** fingerprints, hand topography, hand geometry, retinal and iris recognition
- **What a supplicant produces:** voice and signature patternrecognition

The technology to manage authentication based on what a supplicant knows is widely integrated into the networking and security software systems in use across the IT industry. The last three forms of authentication are usually implemented as some form of identification technology and added to systems that require higher degrees of authentication.

**Authentication**

Authentication is the validation of a supplicant's identity. There are four general ways in which authentication is carried out. Each of these is discussed in detail in the following sections.

**What a Supplicant Knows**

This area of authentication deals with what the supplicant knows- for example , a password , passphrase , or other unique authentication code , such as a personal identification number (orPIN) – that could confirm his or her identity .

A **password** is a private word or combination of characters that only the user should know. One of the biggest debates in the information security industry concerns the complexity of passwords. On the one hand , a password should be difficult to guess, which means it cannot be a series of letters or word that is easily associated with the user, such as the name of theuser's spouse, child, or pet. Nor should a password be a series of numbers commonly associated with the user, such as a phone number , Social Security number, or birth date. On the other hand , the password must be something the user can easily remember, which means it should be short or commonly associated with something the user can remember.

A **passphrase** is a series of characters, typically longer than a password, from which a **virtual password** is derived. For example, which a typical password might be "23skedoo," a typical passphrase can be "May The Force Be With You Always," which can also be represented as "MTFBWYA."

**What a Supplicant Has**

The second area of authentication addresses something the supplicant carries in his or her possession-that is, something they have . These include dumb cards ,such as ID cards or ATM cards with magnetic stripes containing the digital (and often encrypted) user personal identification number (PIN), against which the number a user inputs is compared. An improved version of the dumb card is the smart card, which contains a

computer chip that can verify and validate a number of pieces of information instead of just a PIN. Another device often used is the token, a card or key fob with a computer chip and a liquid crystal display that shows a computer-generated number used to support remote login authentication. Tokens are synchronized with a server, both devices (server and token) use the same time or a time-based database to generate a number that is displayed and entered during the user login phase.

**Asynchronous tokens** use a challenge-response system, in which the server challenges the supplicant during login with a numerical sequence. The supplicant places this sequence into the token and receives a response. The prospective user then enters the response into the system to gain access. This system does not require the synchronization of the synchronous token system and therefore does not require the server and all the tokens to maintain the same exact time setting.

### Who a Supplicant Is

The third area of authentication deals with a characteristic of the supplicant's person that is, something they are. This process of using body measurements is known as biometrics. Biometrics includes:

- Fingerprint comparison of the supplicant's actual fingerprint to a storedfingerprint
- Palm print comparison of the supplicant's actual palm print to a stored palmprint
- Hand geometry comparison of the supplicant's actual hand to a stored measurement
- Facial recognition using a photographic ID card, in which a supplicant's face is compared to a storedimage
- Retinal print comparison of the supplicant's actual retina to a storedimage
- Iris pattern comparison of the supplicant's actual iris to a storedimage

Among all possible biometrics, only three human characteristics are usually considered truly unique:

- Fingerprints
- Retina of the eye (blood vesselpattern)
- Iris of the eye (random pattern of features in the iris including: freckles, pits, striations, vasculature, coronas, andcrypts)

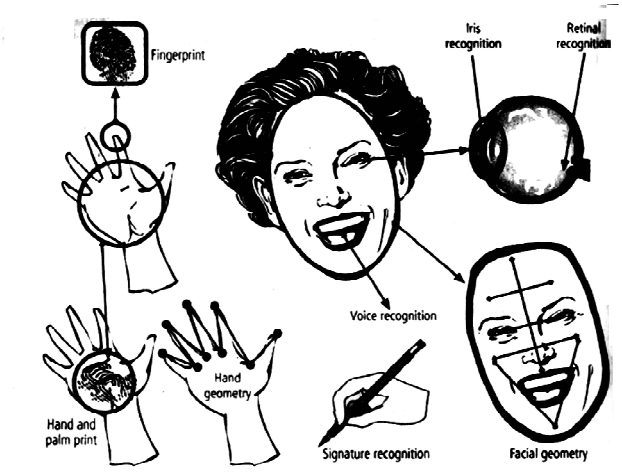
Most of the technologies that scan human characteristics convert these images to some form of minutiae. **Minutiae** are unique points of reference that are digitized and stored in an encrypted format when the user's system access credentials are created. Each subsequent access attempt results in a measurement that is compared with the encoded value to determine if the user is who he or she claims to be. A problem with this method is that some human characteristics can change over time, due to normal development, injury, or illness. This situation requires system designers to create fallback or failsafe authentication mechanisms to be used when the primary biometric procedure fails.

### What a Supplicant Produces

The fourth and final area of authentication addresses something the supplicant performs or something he or she produces. This includes technology in the areas of signature recognition and voice recognition. Signature recognition has become commonplace. Retail stores use signature, or at least signature capture, for authentication during a purchase. The customer signs his or hersignature on a digital pad with a special stylus that captures the signature. The signature isdigitized and either simply saved for future reference, or compared with a signature on a database for validation. Currently, the technology for signature capturing is much more widely accepted than that for signature comparison, because signatures change due to a number of factors, including age, fatigue, and the speed with which the signatures is written.

Voice recognition works in a similar fashion in that an initial voiceprint of the user reciting a phrase is captured and stored. Later, when the user attempts to access the system,the authentication

process will require the user to speak this same phrase so that the technology can compare the current voiceprint against the stored value.




**Biometric Recognition Characteristics**

## Effectiveness of Biometrics

Biometric technologies are evaluated on three basis criteria: first, the reject rate, which is the percentage of supplicants who are in fact authorized users but are denied access; second, the false accept rate, which is the percentage of supplicants who are unauthorized users but are granted access; finally, the crossover error rate, which is the level at which the number of false rejections equals the false acceptances. Each of these is examined in detail in the following sections.

## False Reject Rate

The **false reject rate** is the percentage of or value associated with the rate at which supplicants who are authentic users are denied or prevented access to authorized areas as a result of a failure in the biometric device. This error rate is also known as a Type I error. While a nuisance to supplicants who are authorized users, this error rate is probably the one that least concerns security professionals since rejection of an authorized individual represents no threat to security, but is simply an inpedance to authenticated use. As a result, the false reject rate is often ignored until it increases to a level high enough to irritate supplicants who, subsequently, begin complaining. Most people have experienced the frustration of having a frequently used credit card or ATM card fail to perform because of problems with the magnetic strip. In the field of biometrics, similar problems can occur when a system fails to pick up the various information points it uses to authenticate a prospective userproperly.

## False Accept Rate

The **false accept rate** is the percentage of or value associated with the rate at which supplicants who are not legitimate users are allowed access to systems or areas as a result of a failure in the biometric device. This error rate is also known as a Type II error. This type of error is unacceptable to security professionals, as it represents a clear breach of access.

## Crossover Error Rate(CER)

The **crossover error rate(CER)** is the level at which the number of false rejections equals the false acceptances, also known as the equal error rate. This is possibly the most common and important overall measure of the accuracy of a biometric system. Most biometric systems can be adjusted to compensate for both false positive and false negative errors. Adjustment to oneextreme creates a system that requires

perfect matches and results in high false rejects, but almost no false accepts. Adjustment to the other extreme produces low false rejects, but almost no false accepts. The trick is to find the balance between providing the requisite level of security and minimizing the frustration level of authentic users. Thus, the optimal setting is found to be somewhere near the point at which these two error rates are equal-that is, at the crossover error rate or CER. CERs are used to compare various biometrics and may vary by manufacturer. A biometric device that provides a CER of 1% is a device for which the failure rate for false rejection and the failure rate for false acceptance are identical, at 1% failure of each type. A device with a CER of 1% is considered superior to a device with a CER of 5%.

### Acceptability of Biometrics

As you've learned, a balance must be struck between how acceptable a security system is to its users and how effective it is in maintaining security. Many the biometric systems that are highly reliable and effective are considered somewhat intrusive to users. As a result, many information security professionals, in an effort to avoid confrontation and possible user boycott of the biometric controls, don't implement them. Interestingly, the order of effectiveness is nearly exactly opposite the order of acceptance.

**Ranking of Effectiveness and Acceptance[21]**

| Effectiveness of Biometric Authentication Systems—Ranked from Most Secure to Least Secure | Acceptance of Biometric Authentication Systems—Ranked from Most Accepted to Least Accepted |
|---|---|
| Retina pattern recognition | Keystroke pattern recognition |
| Fingerprint recognition | Signature recognition |
| Handprint recognition | Voice pattern recognition |
| Voice pattern recognition | Handprint recognition |
| Keystroke pattern recognition | Fingerprint recognition |
| Signature recognition | Retina pattern recognition |

## Cryptography

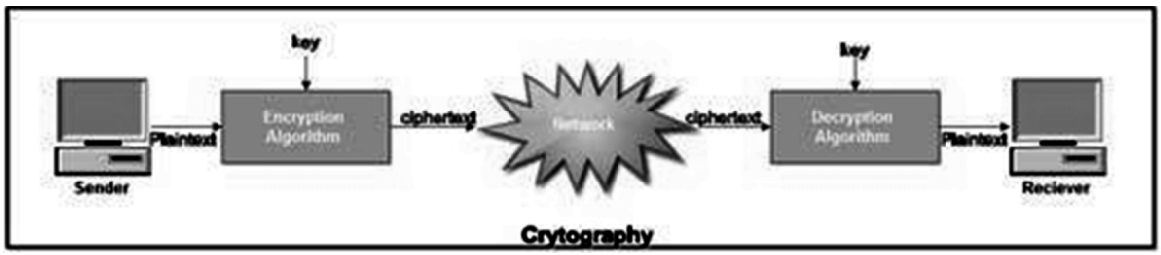
## 4.9 CRYPTOGRAPHY

**Q9. What is cryptography? Define various encryption terms used?**

*Ans :*

### What is Cryptography?

- Cryptography is a technique to provide message confidentiality.
- The term cryptography is a Greek word which means "secret writing".
- It is an art and science of transforming messages so as to make them secure and immune to attacks.
- Cryptography involves the process of encryption and decryption. This process is depicted.



The terminology used in cryptography is given below:

1. **Plaintext.** The original message or data that is fed into the algorithm as input is called plaintext.
2. **Encryption algorithm.** The encryption algorithm is the algorithm that performs various substitutions and transformations on the plaintext. Encryption is the process of changing plaintext into cipher text.
3. **Ciphertext.** Ciphertext is the encrypted form the message. It is the scrambled message produced as output. It depends upon the plaintext and the key.
4. **Decryption algorithm.** The process of changing Ciphertext into plain text is known as decryption. Decryption algorithm is essentially the encryption algorithm run in reverse. It takes the Ciphertext and the key and produces the original plaintext.
5. **Key**. It also acts as input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key. Thus a key is a number or a set of number that the algorithm uses to perform encryption and decryption.

There are two different approaches to attack an encryption scheme:

- Cryptanalysis
- Brute-force attack

**Cryptanalysis**

- The process of attempting to discover the plaintext or key IS known as cryptanalysis.
- The strategy used by cryptanalyst depends on the nature of the encryption scheme and the information available to the cryptanalyst.

**Cryptanalyst can do any or all of six different things:**

- Attempt to break a single message.
- Attempt to recognize patterns in encrypted messages, to be able to break subsequent ones by applying a straight forward decryption algorithm.
- Attempt to infer some meaning without even breaking the encryption, such as noticing an unusual-frequency of communication or determining something by whether the communication was short or long.
- Attempt to deduce the key, in order to break subsequent messages easily.
- Attempt to find weaknesses in the implementation or environment of use encryption.
- Attempt to find general weaknesses in an encryption algorithm without necessarily having intercepted any messages.

**Brute-force attack**

- This method tries every possible key on a piece of Ciphertext until an intelligible translation into plaintext is obtained.
- On an average, half of all possible keys must be tried to achieve the success.

## 4.10 A Short History of Cryptology

**Q10. Explain evolution of cryptology in security systems?**

*Ans :*

The creation and use of cryptology has a long history among the cultures of the world. Table 8.1 provides an overview of the history of cryptosystems.

| Date | Event |
|---|---|
| 1900 B.C. | Egyptian scribes used nonstandard hieroglyphs while inscribing clay tablets; this is the first documented use of written cryptography. |
| 1500 B.C. | Mesopotamian cryptography surpassed that of the Egyptians. This is demonstrated by a tablet that was discovered to contain an encrypted formula for pottery glazes; the tablet used symbols that have different meanings than when used in other contexts. |
| 500 B.C. | Hebrew scribes writing the book of Jeremiah used a reversed alphabet substitution cipher known as ATBASH. |
| 487 B.C. | The Spartans of Greece developed the *skytale*, a system consisting of a strip of papyrus wrapped around a wooden staff. Messages were written down the length of the staff, and the papyrus was unwrapped. The decryption process involved wrapping the papyrus around a shaft of similar diameter. |
| 50 B.C. | Julius Caesar used a simple substitution cipher to secure military and government communications. To form an encrypted text, Caesar shifted the letter of the alphabet three places. In addition to this monoalphabetic substitution cipher, Caesar strengthened his encryption by substituting Greek letters for Latin letters. |
| Fourth to sixth centuries | The *Kama Sutra of Vatsayana* listed cryptography as the 44th and 45th of the 64 arts (yogas) that men and women should practice:*(44) The art of understanding writing in cipher, and the writing of words in a peculiar way; (45) The art of speaking by changing the forms of the word.* |
| 725 | Abu 'Abd al-Rahman al-Khalil ibn Ahman ibn 'Amr ibn Tammam al Farahidi al-Zadi al Yahmadi wrote a book (now lost) on cryptography; he also solved a Greek cryptogram by guessing the plaintext introduction. |
| 855 | Abu Wahshiyyaan-Nabati, a scholar, published several cipher alphabets that were used to encrypt magic formulas. |
| 1250 | Roger Bacon, an English monk, wrote *Epistle of Roger Bacon on the Secret Works of Art and of Nature and Also on the Nullity of Magic*, in which he described several simple ciphers. |

| Date | Event |
|---|---|
| 1392 | *The Equatorie of the Planetis*, an early text possibly written by Geoffrey Chaucer, contained a passage in a simple substitution cipher. |
| 1412 | *Subhalasha*, a 14-volume Arabic encyclopedia, contained a section on cryptography, including both substitution and transposition ciphers, as well as ciphers with multiple substitutions, a technique that had never been used before. |
| 1466 | Leon Battista Alberti, the Father of Western cryptography, worked with polyalphabetic substitution and also designed a cipher disk. |
| 1518 | Johannes Trithemius wrote the first printed book on cryptography and invented a steganographic cipher, in which each letter was represented as a word taken from a succession of columns. He also described a polyalphabetic encryption method using a rectangular substitution format that is now commonly used. He is credited with introducing the method of changing substitution alphabets with each letter as it is deciphered. |
| 1553 | Giovan Batista Belaso introduced the idea of the passphrase (password) as a key for encryption; this polyalphabetic encryption method is misnamed for another person who later used the technique and is called "The Vigenère Cipher" today. |
| 1563 | Giovanni Battista Porta wrote a classification text on encryption methods, categorizing them as transposition, substitution, and symbol substitution. |
| 1623 | Sir Francis Bacon described an encryption method employing one of the first uses of steganography; he encrypted his messages by slightly changing the type-face of a random text so that each letter of the cipher was hidden within the text. |
| 1790s | Thomas Jefferson created a 26-letter wheel cipher, which he used for official communications while ambassador to France; the concept of the wheel cipher would be reinvented in 1854 and again in 1913. |
| 1854 | Charles Babbage reinvented Thomas Jefferson's wheel cipher. |
| 1861–5 | During the U.S. Civil War, Union forces used a substitution encryption method based on specific words, and the Confederacy used a polyalphabetic cipher whose solution had been published before the start of the Civil War. |
| 1914–17 | During World War I, the Germans, British, and French used a series of transposition and substitution ciphers in radio communications throughout the war. All sides expended considerable effort to try to intercept and decode communications, and thereby created the science of cryptanalysis. British cryptographers broke the Zimmerman Telegram, in which the Germans offered Mexico U.S. territory in return for Mexico's support. This decryption helped to bring the United States into the war. |
| 1917 | William Frederick Friedman, the father of U.S. cryptanalysis, and his wife, Elizabeth, were employed as civilian cryptanalysts by the U.S. government. Friedman later founded a school for cryptanalysis in Riverbank, Illinois. |
| 1917 | Gilbert S. Vernam, an AT&T employee, invented a polyalphabetic cipher machine that used a nonrepeating random key. |
| 1919 | Hugo Alexander Koch filed a patent in the Netherlands for a rotor-based cipher machine; in 1927, Koch assigned the patent rights to Arthur Scherbius, the inventor of the Enigma machine, which was a mechanical substitution cipher. |
| 1927–33 | During Prohibition, criminals in the U.S. began using cryptography to protect the privacy of messages used in criminal activities. |

| Date | Event |
|---|---|
| 1937 | The Japanese developed the Purple machine, which was based on principles similar to those of Enigma and used mechanical relays from telephone systems to encrypt diplomatic messages. By late 1940, a team headed by William Friedman had broken the code generated by this machine and constructed a machine that could quickly decode Purple's ciphers. |
| 1939–42 | The Allies secretly broke the Enigma cipher, undoubtedly shortening World War II. |
| 1942 | Navajo code talkers entered World War II; in addition to speaking a language that was unknown outside a relatively small group within the United States, the Navajos developed code words for subjects and ideas that did not exist in their native tongue. |
| 1948 | Claude Shannon suggested using frequency and statistical analysis in the solution of substitution ciphers. |
| 1970 | Dr. Horst Feistel led an IBM research team in the development of the Lucifer cipher. |
| 1976 | A design based upon Lucifer was chosen by the U.S. National Security Agency as the Data Encryption Standard and found worldwide acceptance. |
| 1976 | Whitefield Diffie and Martin Hellman introduced the idea of public-key cryptography. |
| 1977 | Ronald Rivest, Adi Shamir, and Leonard Adleman developed a practical public-key cipher for both confidentiality and digital signatures; the RSA family of computer encryption algorithms was born. |
| 1978 | The initial RSA algorithm was published in the Communication of ACM. |
| 1991 | Phil Zimmermann released the first version of PGP (Pretty Good Privacy); PGP was released as freeware and became the worldwide standard for public cryptosystems. |
| 2000 | Rijndael's cipher was selected as the Advanced Encryption Standard. |

## 4.11 Principles of Cryptography

**Q11. List few crypto system principles?**

*Ans :*

Historically, cryptography was used in manual applications, such as handwriting. But with the emergence of automated technologies in the 20th century, the need for encryption in the IT environment vastly increased. Today, many common IT tools use embedded encryption technologies to protect sensitive information within applications. For example, all the popular Web browsers use built -in encryption features that enable users to perform secure e-commerce applications, such as online banking and Web shopping.

**Basic Encryption Definitions**

To understand the fundamentals of cryptography, you must become familiar with the following definitions:

- **Algorithm:** The programmatic steps used to convert an unencrypted message into an encrypted sequence of bits that represent the message; sometimes used as a reference to the programs that enable the cryptographic processes.
- **Cipher or cryptosystem:** An encryption method or process encompassing the algorithm, key(s) or cryptovariable(s), and procedures used to perform encryption anddecryption
- **Ciphertext or cryptogram:** The unintelligible encrypted or encoded message resulting from anencryption
- **Code:** The process of converting components (words or phrases) of an unencrypted message into encrypted components
- **Decipher:** To decrypt or convert ciphertext into the equivalentplaintext
- **Encipher:** To encrypt or convert plaintext into the equivalentciphertext
- **Key or cryptovariable:** The information used in conjunction with an algorithmto

- create the ciphertext from the plaintext or derive the plaintext from the ciphertext; the key can be a series of bits used by a computer program, or it can be a passphrase used by humans that is then converted into a series of bits for use in the computerprogram
- **Keyspace:** The entire range of values that can possibly be used to construct an individual key
- **Link encryption:** A series of encryptions and decryptions between a number of systems, wherein each system in a network decrypts the message sent to it and then reencrypts it using different keys and sends it to the next neighbor, and this process continues until the message reaches the final destination
- **Plaintext or cleartext:** The original unencrypted message that is encrypted; also the name given to the results of a message that has been successfully ecrypted
- **Steganography:** The process of hiding messages-for example, messages can be hidden within the digital encoding of a picture orgraphic
- **Work factor:** The amount of effort (usually in hours) required to perform cryptanalysis on an encoded message so that it maybe decrypted when the key or algorithm (or both)
- are unknown

## 4.12 CIPHER METHODS

**Q12. What are the different possible attacks on crypto system? Explain with either methods.**

*Ans :*

A plaintext can be encrypted through one of two methods, the bit stream method or the block cipher method. With the bit stream method, each bit in the plaintext is transformed into a cipher bit one bit at a time. In the case of the block cipher method, the message is divided into blocks, for example, sets of 8-,16-,32-, or 64-bit blocks, and then each block of plaintext bits is transformed into an encrypted block of cipher bits using an algorithm and a key. Bit stream methods most commonly use algorithm functions like the exclusive OR operation (XOR), whereas block methods can use substitution, transposition, XOR, or some combination of these operations, as described in the following sections. As you read on, you should note that most encryption methods using computer systems will operate on data at the level of its binary digits (bits), but SOme operations may operate at the byte or character level.

**Elements of Cryptosystems**

Cryptosystems are made up of a number of elements or components. These are usually algorithms and data handling techniques as well as procedures and process steps, which are combined in multiple ways to meet a given organization's need to ensure confidentiality and provide specialized authentication and authorization for its business processes. In the sections that follow, you will first read about the technical aspects of a number of cryptographic techniques, often called ciphers. The chapter will continue with an exploration of some of the tools commonly used to implement cryptographic systems in the world of business. The discussion will then proceed to the security protocols used to bring communications security to the Internet and the world of e-commerce. Finally, the chapter will conclude with a discussion of the attacks that are often found being used against cryptosystems. Along the way, you will also encounter a number of Technical Details boxes that cover advanced material. Be sure to check with your instructor about how your course will include the Technical Detailsmaterial.

**Substitution Cipher**

When using a **substitution cipher,** you substitute one value for another. For example, you can substitute a letter in the alphabet with the letter three values to the right. Or, you may substitute one bit for another bit that is four places to its left. A three-character substitution to the right would result in the following transformation of the standard English alphabet:

**Initialalphabet** **ABCDEFGHIJKLMNOPQRSTUVWXYZ** yields
**Encryptionalphabet** **DEFGHIJKLMNOPQRSTUVWXYZABC**

Within this substitution scheme, the plaintext MOM would be encrypted into the ciphertextPRP.

This is a simple enough method by itself but very powerful if combined with other operations. Incidentally, this type of substitution is based on a monoalphabetic substitution, since it only uses one alphabet. More advanced substitution ciphers use two or more alphabets, and are referred to as polyalphabetic substitutions.

To continue the previous example, consider the following block of text:

Plaintext = ABCDEFGHIJKLMNOPQRSTUVWXYZ

**1st Substitution cipher 1 = DEFGHIJKLMNOPQRSTU**~YZABC

**2nd Substitution cipher 2 =** GHIJKLMNOPQRSTUVWXYZABCDEF

**3rd Substitution cipher 3 =** JKLMNOPQRSTUVWXYZABCDEFGHI

**4th Substitution cipher 4 =** MNOPQRSTUVWXYZABCDEFGHIJKL

The first row here is the plaintext, and the next four rows are four sets of substitution ciphers, which taken together constitute a single polyalphabetic substitution cipher. To encode the word TEXT with this cipher, you substitute a letter from the second row for the first letter in TEXT, a letter from the third row for the second letter, and so on-a process that yields the ciphertext WKGF. Note how the plaintext letter T is transformed into a W or a F, depending on its order of appearance in the plaintext. Complexities like these make this type of encryption substantially more difficult to decipher when one doesn't have the algorithm (in this case, the rows of ciphers) and the key, which is the method used (in this case the use of the second row for first letter, third for second, and so on). A logical extension to this process would be to randomize the cipher rows completely in order to create a more complex operation.

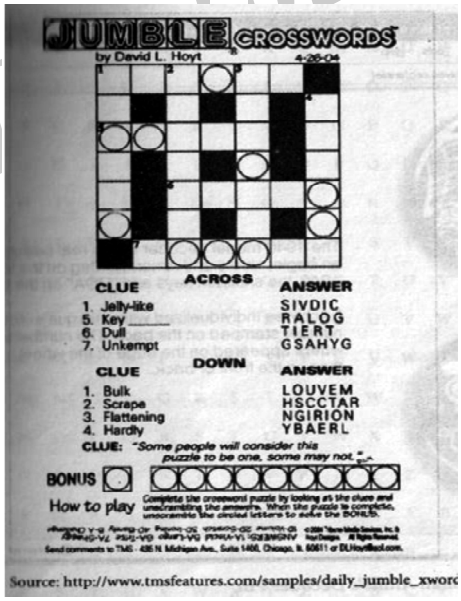
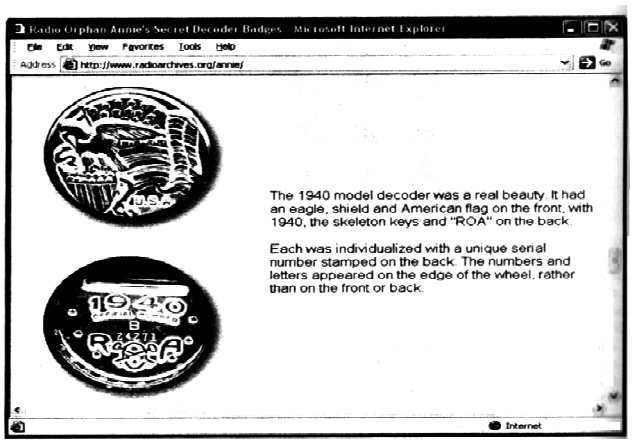



**Fig: Daily cryptogram**

One example of a substitution cipher is the cryptogram in the daily newspaper; another is the once famous Radio Orphan Annie decoder pin, which consisted of two alphabetic rings that could be rotated to a predetermined pairing to form a simple substitution cipher. The device was made to be worn as a pin so one could always be at the ready. Caesar reportedly used a three-position shift to the right to encrypt his messages (so A became D, B became E, and so on), thus this particular substitution cipher was given his name-the CaesarCipher.




**Radio Orphan Annie's Decoder Pin**

An advanced type of substitution cipher that uses a simple polyalphabetic code is the Vigenere cipher. The cipher is implemented using the Vigenere Square. which is made up of 26 distinct cipher alphabets. The setup of the Vigenere Square. In the header row, the alphabet is written in its normal order. In each subsequent row, the alphabet is shifted one letter to the right until a 26 X 26 block of letters is formed. There are a number of ways to use the Vigenere square. You could perform an encryption by simply starting in the first row and finding a substitute for the first letter of plaintext, and then moving down the rows for each subsequent letter of plaintext. With this method, the word SECURITY in plaintext would become TGFYWOAG inciphertext.

**The Vigenère Square**

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| 2 | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| 3 | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| 4 | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| 5 | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| 6 | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| 7 | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| 8 | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| 9 | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| 10 | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| 11 | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| 12 | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| 13 | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| 14 | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| 15 | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 16 | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| 17 | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| 18 | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| 19 | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| 20 | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| 21 | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| 22 | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| 23 | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| 24 | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| 25 | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

A much more sophisticated way to use the Vigènere Square would be to use a keyword to represent the shift. To accomplish this, you would begin by writing a keyword above the plaintext message. For example, suppose the plaintext message was "SACK GAUL SPARE NO ONE" and the keyword was ITALY. We thus end up with the Following :

**ITALYITALYITALYITA èè SACKGAULSPARENOONE**

The idea behind this is that you will now use the keyword letter and the message (plaintext)letter below it in combination. Returning to the Vigenere Square, notice how the first column of text, like the first row, forms the normal alphabet. To perform the substitution of the message, start with first combination of keyword and message letters, IS. Use the keyword letter to locate the column, and the message letter to find the row, and then look for the letter at their intersection. Thus, for column "I" and row "S," you will find the ciphertext letter ''JI". After you follow this procedure for each of the letters in the message, you will produce the encrypted ciphertext ATCVEINLDNIKEYMWGE. Curiously, one weakness of this method is that any keyword-message letter combination containing an *"N'* row or column will reproduce the plaintext message letter. For example, the third letter in the plaintext message, the C (of SACK), has a combination of AC, and thus is unchanged in the ciphertext. To minimize the effects of this weakness, you should avoid choosing a keyword that contains the letter "A."

**Transposition Cipher**

The next type of cipher operation is the transposition. Just like the substitution operation, the transposition cipher is simple to understand, but it can, if properly used, produce ciphertext that is complex to decipher. In contrast to the substitution cipher, however, the **transposition cipher** (or **permutation cipher)** simply rearranges the values within a block to create the ciphertext. This can be done at the bit level or at the byte (character) level. For an example, consider the following transposition keypattern.

**Key pattern:**

**1-4, 2-8, 3-1, 4-5, 5-7, 6-2, 7-6, 8-3**

In this key, the bit or byte (character) in position 1 (with position 1 being at the far right) moves to position 4 (counting from the right), and the bit or byte in position 2 moves to position 8, and so on.

The following rows show the numbering of bit locations for this key; the plaintext message **00100101011010111001010101010100**, which is broken into 8-bit blocks for ease of discussion; and the ciphertext that is produced when the transposition key depicted above is applied to the plaintext:

| | | |
|---|---|---|
| **Bit locations:** | 87654321 8765432187654321 | 87654321 |
| **Plaintext 8-bit blocks:** | 00100101 0110101110010101 | 01010100 |
| **Ciphertext:** | 00001011 1011101001001101 | 01100001 |

Reading from right to left in the example above, the first bit of plaintext (position 1 of the first byte) becomes the fourth bit (in position 4) of the first byte of the ciphertext. Similarly, the second bit of the plaintext (position 2) becomes the eighth bit (position 8) of the ciphertext, and "soon.

To examine further how this transposition key works, let's see its effects on a plaintext message comprised of letters instead of bits. Replacing the 8-bit block of plaintext with the example plaintext message presented earlier, "SACK GAUL SPARE NO ONE," yields the following:

**Letterlocations:** 87654321 87654321 87654321

**Plaintext:** SACKGAUL SPARENOO NE

**Key:** Same key as above, but characters transposed, notbits.

**Ciphertext:** UKAGLSCA ORPEOSAN EN

Here, reading again from right to left, the letter in position I of the first block of plaintext, "I.:', becomes the letter at position 4 in the ciphertext. In other words, the "L" that is the 8'h letter of the plaintext is the ''L'' at the 5th letter of the ciphertext. The letter in position 2 of the first block of plaintext, "U': becomes the letter at position 8 in the ciphertext. In other words, the "U" that is the 7th letter of the plaintext is the "U" at the 151 letter of the ciphertext. This process continues using the specified pattern.

In addition to being credited with inventing a substitution cipher, Julius Caesar was associated with an early version of the transposition cipher. As part of the Caesar block cipher, a courier would carry a message that when read normally would be unintelligible. However, the receiver of the message would know to fit the text to a prime number square (in practice, this meant that if there were fewer than 25 characters, the receiver would use a 5 x 5 square). For example,suppose you were the receiver and the ciphertext shown below arrived at your doorstep. Since it was from Caesar, you would know to make a square of 5 columns and 5 rows, and then to write the letters of the message into the square, filling the slots from left to right, top to bottom. Also, when you'd finished doing this, you'd know to read the message the opposite direction-that is, from top to bottom, left toright.

**Ciphertext:** SGS-NAAPNECUAO KLR EO S G S - NA A P N E C U A 0K L R_—_-_E O-

Reading from top to bottom, left to right reveals the plaintext "SACK GAUL SPARE NO ONE':

When mechanical and electronic cryptosystems became more widely used, transposition ciphers and substitution ciphers began to be used in combinations to produce highly secure encryption processes. To make the encryption even stronger (more difficult to cryptanalyze) the keys and block sizes can be made much larger (up to 64 or 128 bits in size), which produces substantially more complex substitutions or transpositions.

## 4.13 EXCLUSIVE OR

**Q13. Explain in detail about?**

**(a) Exclusive –OR (b) Vigenere cipher (c) Book (or) Running key cipher.**

*Ans :*

The **exclusive OR operation** (XOR) is a function of Boolean algebra in which two bits are compared, and if the two bits are identical, the result is a binary O. If the two bits are not the same, the result is a binary 1. XOR encryption is a very simple symmetric cipher that is used in many applications where security is not a defined requirement a truth table for XOR with the results of all the possible combinations of two bits.

**XOR Truth Table**

| First Bit | Second Bit | Result |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

To see how XOR works, let's consider an example in which the plaintext we will start with is the word "CAT': The binary representation of the plaintext is "0 1110000 01100101 1000000". In order to encrypt the plaintext, a key value should be selected. In this case, the bit pattern for the letter "Y" (10000101) will be used and repeated for each character to be encrypted. Performing the XOR operation on the two bit streams will produce thefollowing result:

**Example XOR Encryption**

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CAT as bits | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| vvv as key | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| cipher | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |

The row of labeled "Cipher" contains the bit stream that will be transmitted; when this cipher is received, it can be decrypted using the key value of "y"'. Note that the XOR encryption method is very simple to implement and equally simple to break. The XOR encryption method should not be used by itself when an organization is transmitting or storing data that needs protection. Actual encryption algorithms used to protect data typically use the XOR operator as part of a more complex encryption process, thus understanding XOR encryption is a necessary step on the path to becoming a cryptologist.

Often, one can combine the XOR operation with a block cipher operation to produce a simple but powerful operation. Consider the example that follows, the first row of which shows a character message "5E5+'" requiring encryption. The second row shows this message in binary notation. In order to apply an 8-bit block cipher method, the binary message is broken into 8-bit blocks in therow labeled "Message Blocks."The fourth row shows the 8-bit key (01010101) chosen for the encryption; To encryptthe message, you must perform the XOR operation on each 8-bit block by using the XOR function on the message bit and the key bit to determine the bits of the ciphertext until the entire message is enciphered. The result is shown in the row labeled "Ciphertext': This ciphertext can now be sent to a receiver, who will be able to decipher the message by simply knowing the algorithm (XOR) and the key (01010101).

**Message (text)** : "5E5+"

**Message (binary)** : 00110010100010100110101001010111001010 1

**Message blocks** : 00110101 01000101 00110101 00101011 10010101

**Key** : 01010101 01010101 01010101 01010101 01010101

**Ciphertext** : 01100000 00010000 01100000 01111110 11000000

If the receiver cannot apply the key to the ciphertext and derive the original message, either the cipher was applied with an incorrect key or the cryptosystem was not used correctly.

### 4.13.1 Vernam Cipher

This scheme of cipher uses a text string (say, a word) as a key, which is then used for doing a number of shifts on the plaintext.

For example, let's assume the key is 'point'. Each alphabet of the key is converted to its respective numeric value: In this case,

$p \rightarrow 16$, $o \rightarrow 15$, $i \rightarrow 9$, $n \rightarrow 14$, and $t \rightarrow 20$.

Thus, the key is: 16 15 9 14 20.

**Process of Vigenere Cipher**

- The sender and the receiver decide on a key. Say 'point' is the key. Numeric representation of this key is '16 15 9 14 20'.
- The sender wants to encrypt the message, say 'attack from south east'. He will arrange plaintext and numeric key as follows.

| a | t | t | a | c | k | f | r | o | m | s | o | u | t | h | e | a | s | t |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 |

- He now shifts each plaintext alphabet by the number written below it to create ciphertext as shown below

| a | t | t | a | c | k | f | r | o | m | s | o | u | t | h | e | a | s | t |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 |
| Q | I | C | O | W | A | U | A | C | G | I | D | D | H | B | U | P | B | H |

- Here, each plaintext character has been shifted by a different amount – and that amount is determined by the key. The key must be less than or equal to the size of the message.
- For decryption, the receiver uses the same key and shifts received ciphertext in reverse order to obtain the plaintext.

| Q | I | C | O | W | A | U | A | C | G | I | D | D | H | B | U | P | B | H |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 | 20 | 16 | 15 | 9 | 14 |
| a | t | t | a | c | k | f | r | o | m | s | o | u | t | h | e | a | s | t |

**Security Value**

Vigenere Cipher was designed by tweaking the standard Caesar cipher to reduce the effectiveness of cryptanalysis on the ciphertext and make a cryptosystem more robust. It is significantly **more secure than a regular Caesar Cipher**.

In the history, it was regularly used for protecting sensitive political and military information. It was referred to as the **unbreakable cipher** due to the difficulty it posed to the cryptanalysis.

### 4.13.2 Variants of Vigenere Cipher

There are two special cases of Vigenere cipher

- The keyword length is same as plaintect message. This case is called **Vernam Cipher**. It is more secure than typical Vigenere cipher.
- Vigenere cipher becomes a cryptosystem with perfect secrecy, which is called **One-time pad**.

**One-Time Pad**

The circumstances are:

- The length of the keyword is same as the length of the plaintext.
- The keyword is a randomly generated string of alphabets.
- The keyword is used only once.

**Security Value**

Let us compare Shift cipher with one-time pad.

**Shift Cipher " Easy to Break**

In case of Shift cipher, the entire message could have had a shift between 1 and 25. This is a very small size, and very easy to brute force. However, with each character now having its own individual shift between 1 and 26, the possible keys grow exponentially for the message.

**One-time Pad - Impossible to Break**

Let us say, we encrypt the name "point" with a one-time pad. It is a 5 letter text. To break the ciphertext by brute force, you need to try all possibilities of keys and conduct computation for (26 × 26

× 26 × 26 × 26) = $26^5$ = 11881376 times. That's for a message with 5 alphabets. Thus, for a longer message, the computation grows exponentially with every additional alphabet. This makes it computationally impossible to break the ciphertext by brute force.

### 4.13.3 Book or Running Key Cipher

One encryption method made popular by spy movies involves using the text in a book asthe key to decrypt a message. The ciphertext consists of a list of codes representing thepage number, line number, and word number of the plaintext word. The algorithm is themechanical process of looking up the references from the ciphertext and converting eachreference to a word by usingthe ciphertext's value and the key (the book). For example,from a copy of a particular popular novel, one may send the message: 259,19,8; 22,3,8;375,7,4; 394,17,2. Although almost any book will work just fine, dictionaries andthesauruses are typically the most popular sources as they can guarantee having almostevery word that might be needed. Returning to the example, the receiver must first knowwhich novel is used-in this case, suppose it is the science fiction novel, A Fire Upon theDeep, the 1992 TOR edition. To decrypt the ciphertext, the receiver would acquire the book and begin by turning to page 259, finding line 19, and selecting the eighth word inthat line (which happens to be "sack"). Then the receiver would go to page 22, line 3, andselect the eighth word again, and so forth. For this example, the resulting message will be"SACK IS LAND SHARP PATH". If dictionaries are used, the message would be made up of only the page number and the number of the word on the page. An even more sophisticated version might use multiple books, perhaps even in a particular sequence for each word orphrase

### Hash Functions

In addition to ciphers, another important encryption technique that is often incorporated into cryptosystems is the hash function. Hash functions are mathematical algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm the identity of a ~pacific message and to confirm that there have not been any changes to the content While not directly related to the creation of a ciphertext, hash functions are used to confirm message identity and integrity, both of which are critical functions in e-commerce.

Hash algorithms are publicly known functions that create a hash value, also known as a message digest, by converting variable-length messages into a single fixed-length value. The message digest is a fingerprint of the author's message that is to be compared with the receiver's locally calculated hash of the same message If both hashes are identical after transmission, the message has arrived without modification. Hash functions are considered one-way operations in that the message will always provide the same hash value if it is the same message, but the hash value itself cannot be used to determine the contents of the message.

Hashing functions do not require the use of keys, but a message authentication code(MAC), which is a key-dependent, and one-way hash function, may be attached to a message to allow only specific recipients to access the message digest The MAC is essentially a one-wayhashvalue that is encrypted with a symmetric key. The recipients must possess the key to access themessage digest and to confirm message integrity.

Because hash functions are one-way, they are used in password verification systems to confirm the identity of the user. In such systems, the hash value, or message digest, is calculated based upon the originally issued password, and this message digest is storedfor later comparison. When the user logs on for the next session, the system calculates a hash value based on the user's inputted password. The newly calculated hash value is compared against the stored value to confirmidentity.

The Secure Hash Standard (SHS) is a standard issued by the National Institute of Standards and Technology (NIST). Standard document FIPS 180-1 specifies SHA-l (Secure Hash Algorithm 1) as a secure algorithm for computing a condensed representation of a message or data file. SHA-I produces a 160-bit message digest, which can then be used as an input to a digital signature algorithm. SHA-I is based on principles modeled after MD4 (which is part of the

MDxfamily of hash algorithms created by Ronald Rivest). New hash algorithms (SHA-256, SHA-384, and SHA-512) have been proposed by

NIST as standards for 128, 192, and 156 bits, respectively. The number of bits used in the hash algorithm is a measurement of the strength of the algorithm against collision attacks. SHA-256 is essentially a 256-bit block cipher algorithm that creates a key by encrypting the intermediate hash value with the message block functioning as the key. The compression function operates on each 512-bit message block and a 256-bit intermediate message digest'

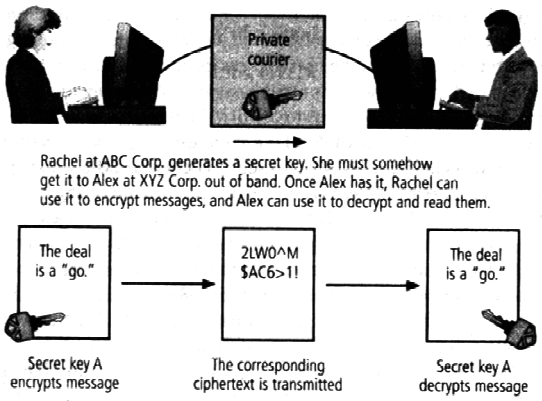
## 4.14 Cryptographic Algorithms

**Q14. Explain different cryptographic algorithms in detail?**

*Ans :*

In general, cryptographic algorithms are often grouped into two broad categories-symmetric and asymmetric-but in practice, today's popular cryptosysterns use a hybrid combination of symmetricand asymmetric algorithms. Symmetric and asymmetric algorithms can be distinguished by the types of keys they use for encryption and decryption operations. The upcoming section discusses both of these algorithms, and includes Technical Details boxes that provide supplemental information on cryptographic notation and advanced encryption standards.

Symmetric Encryption- A method of encryption that requires the same secret key to encipher and decipher the message is known as private key encryption or symmetric encryption. Symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms so that the encryption and decryption processes are done quickly by even small computers. As you can see in Figure 8- 3, one of the challenges is that both the sender and the receiver must have the secret key. Also, if either copy of the key falls into the wrong hands, messages can be decrypted by others and the sender and intended receiver may not know the message was intercepted. The primary challenge of symmetric key encryption is getting the key to the receiver, a process that must be conducted out of band to avoid interception.




**Example of Symmetric Encryption**

### Cryptographic Notation

The notation used to describe the encryption process varies, depending on its source. The notation chosen for the discussion in this text uses the letter M to represent the original message, C to represent the ending ciphertext, and E to represent the encryption process: thus, $E(M) = C^2$ This formula represents the application of encryption (E) to a message (M) to create ciphertext (C). Also in this notation scheme, the letter D represents the decryption or deciphering process, thus the formula D[E(M)] = M states that if you decipher (D) an enciphered an message (E(M)), you should get the original message (M). This could also be stated as D[C] = M, or the deciphering of the ciphertext (remember that C = E(M)) results in the original message M. Finally the letter K is used to represent the key, therefore(M,K) = C suggests that encrypting (E) the message (M) with the key (K) results in the ciphertext (C). Similarly, D(C,K) = D[E(M,K),K] = M, or deciphering the ciphertext with key K results in the original plaintext message—or, to translate this formula even more precisely, deciphering with key K the message encrypted with key K results in the originalmessage.

To encrypt a plaintext set of data, you can use one of two methods: bit stream and block cipher. With the bit stream method, the message is divided into blocks, e.g., 8, 16, 32, or 64-bit blocks, and then each block is transformed using the algorithm and key. Bit stream methods most commonly use algorithm functions like XOR, whereas block methods can use XOR, transposition, or substitution.

There are a number of popular symmetric encryption cryptosystem. One of the most widely

known is the DATA ENCRYPTION STANDARS (DES)., which was developed by IBM and is based on the company's Lucifer algorithm, which uses a key length of 128 bits. Asimplemented, DES uses a 64-bit block size and a 56-bit key.DES was adopted by NIST in 1976 as a federal standard for encryption of non-classified information.With this approval, DES became widely employed in commercial applications as the encryption standard of choice. DES enjoyed increasing popularity for almost 20 years, until 1997, when users realized that using a 56-bit key size was no longer sufficient as an acceptable level of secure communications. And soon enough, in 1998, a group called Electronic Frontier Foundation, using a specially designed computer, broke a DES key in less than three days(just over 56 hours, to be precise). Since then,it has been theorized that a dedicated attack supported by the proper hardware (thus , not even a specialized computer like that of Electronic Frontier Foundation) can break a DES key in less than fourhours.

As DES became known as being too weak for highly classified communications, Triple DES (3DES) was created to provide a level of security far beyond that of DES. 3 DES was an advanced application of DES, and was in fact originally designed to replace DES. While 3DES did deliver on its promise of encryption strength beyond DES, it too was soon proven too weak to survive indefinitely-especially as computing power continued to double every 18 months. Within just few years, 3DES needed to bereplaced.

## TRIPLE DES (3DES)

As it was demonstrated that DES was not strong enough for highly classified communication, 3DES was created to provide a level of security far beyond that of standard DES.(In between , there was a 2DES; however, it was statistically shown that the double DES did not providesignificantly stronger security than that of DES). 3DES takes three 64-bit keys for an overall key length of 192 bits.Triple DES encryption is the same as that of standard DES; however, it is repeated three times. Triple DES can be employed using two or three keys, and a combination of encryption or decryption to obtain additional security.The most common implementations involve encrypting and /or decrypting with two or three different keys, a process that is described below. 3DES employs 48 rounds in its encryption computation, generating ciphers that are approximately $2^{56}$. (72 quadrillion) times stronger than standard DES ciphers but require only three times longer toprocess.

One example of 3DES encryption is illustrated here:

1. In the first operation, 3DES encrypts the message with key 1, then decrypts it with key 2, and then it encrypts it again with key 1. In cryptographic notation terms, this would be [E{D[E(M,K1)],K2},K1]. Decrypting with a different key is essentially another encryption, but it reverses the application of the traditional encryption operations.
2. In the second operation, 3DES encrypts the message with key 1, then it encrypts it again with key 2, and then it encrypts it a third time with key 1 again, or [E{E[E(M,K1)],K2},K1].
3. In the third operation, 3DES encrypts the message three times with three different keys; [E{E[E(M,K1)],K2},K3].This is the most secure level of encryption possible with3DES.

The successor to 3DES is Advanced Encryption Standard (AES). AES is a Federal Information Processing Standard (FIPS) that specifies a cryptographic algorithm that is used within the U.S. government to protect information at federal agencies that are not a part of the national defense infrastructure. (Agencies that are considered a part of national defense use other, more secure methods of encryption, which are provided by the National Security Agency.) The requirements for AES stipulate that the algorithm should be unclassified, publicly disclosed, and available royalty-free worldwide. AES has been developed to replace both DES and 3DES. While 3DES remains an approved algorithm for some uses, its expected useful life is limited. Historically, cryptographic standards approved by FIPS have been adopted on a voluntary basis by organizations outside government entities. The AES selection process involved cooperation between the U.S. government, private industry, and academia from around the world. AES was approved by the Secretary of Commerce as the official federal governmental standard on May 26,2002.

The AES implements a block cipher called the Rijndael Block Cipher with a variable block length and a key length of 128, 192, or 256 bits. Experts estimate that the special computer used by the Electronic Frontier Foundation to crack DES within a couple of days would require approximately 4,698,864 quintillion years (4,698, 864, 000, 000, 000, 000, 000) to crack AES. To learn more about the AES, See the Technical Details box entitled "Advanced Encryption Standard (AES)."

**Advanced Encryption Standard (AES)**

Of the many ciphers that were submitted (from across the world) for consideration in the AES selection process, five finalists were chosen: MARS, RC6, Rijndael, Serpent, and Twofish. On October 2, 2000, NIST announced the selection of Rijndael as the cipher to be used as the basis for the AES, and this block cipher was approved by the Secretary of Commerce as the official federal governmental standard as of May 26, 2002.

The AES version of Rijndael can use a multiple round based system. Depending on the key size, the number of rounds varies between 9 and 13: for a l28.bit key, 9 rounds plus one end round are used; for a 192-bit key, 11 rounds plus one end round are used; and for a 256-bit key, 13 rounds plus one end round are used. Once Rijndael was adopted as the AES, the ability to use variable sized blocks was standardized to a single l28-bit block forsimplicity.

There are four steps within each Rijndael round, and these are described in "The Advanced Encryption Standard (Rijndael)" by John Savard as follows:

1. The Byte Sub step. Each byte of the block is replaced by its substitute in anS-box
2. (Substitution box). [Author's Note: The S-box consists of a table of computed values, the calculation of which is beyond the scope of this text.]
3. The Shift Row step. Considering the block to be made up of bytes 1 to 16, these bytes are arranged in a rectangle, and shifted asfollows:

| | from | | To |
|---|---|---|---|
| 1 | 5 9 | 13 | 1 5 9 13 |
| 2 | 6 10 | 14 | 6 10 142 |
| 3 | 7 11 | 15 | 11 15 37 |
| 4 | 8 12 | 16 | 16 4 8 12 |

Other shift tables are used for larger blocks.

**MixColumns**

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

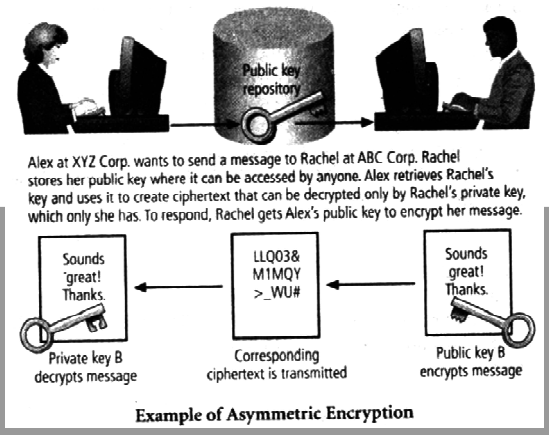
**Addroundkey**

The 16 bytes of the matrix are now considered as 128 bits and are XOR to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Asymmetric Encryption.Another category of encryption techniques is asymmetric encryption. Whereas the symmetric encryption systems are based on using a single key to both encrypt and decrypt a message, asymmetric encryption uses two differentbut related keys, and either key can be used to encrypt or decrypt the message. If, however, Key A is used to encrypt the message, only Key B can decrypt it, and if Key B is used to encrypt a message, only Key A can decrypt it. Asymmetric encryption can be used to provide elegant solutions to problems of secrecy and verification. This technique has its highest value when one key is used as a private key, which means that it is kept secret (much like the key of symmetric encryption), known only to the owner of the key pair, and the other key serves as a public key, which means that it is stored in a public location where anyone can use it. This is why the more common name for asymmetric encryption is public key encryption.

Consider the following example, Alex at XYZ Corporation wants to send an encrypted message to Rachel at ABC Corporation. Alex goes to a public

key registry and obtains Rachel's public key. Remember that the foundation of asymmetric encryption is that the same key cannot be used to both encrypt and decrypt the same message. So.when Rachel's public key is used to encrypt the message, only Rachel's private key can be used to decrypt the message and that private key is held by Rachel alone. Similarly, if Rachel wants to respond to Alex's message, she goes to the registry where Alex's public key is held, and uses it to encrypt her message, which of course can only be read by Alex's private key. This approach, which keeps private keys secret and encourages the sharing of public keys in reliable directories, is an elegant solution to the key management problems found in symmetric key applications.



Example of Asymmetric Encryption

Asymmetric algorithms are based on one-way functions. A one-way function is simple to compute in one direction, but complex to compute in the opposite. This is the foundation of public-key encryption. Public-key encryption is based on a hash value, is calculated from an input number using a hashing algorithm. This hash value is essential summary of the original input values. It is virtually impossible to derive the original values without knowing how the values were used to create the hash value. For example.if you multiply 45 by 235 you get 10,575. This is simple enough. But if you are simply given the number 10,575, can you determine which two numbers were multiplied to determine this number? Now assume that each multiplier is 200 digits long and prime. The resulting multiplicative product would be up to 400 digits long. Imagine the time you'd need to factor that out There is a shortcut, however. In mathematics, it is known as a trapdoor (which is different from the software trapdoor). A mathematical trapdoor is a "secret mechanism that enables you to easily accomplish the reverse function in a one-way function" 4 With a trapdoor, you can use a key to encrypt or decrypt the ciphertext, but not both, thus requiring two keys. The public key becomes be the true key, and the private key is to be derived from the public key using the trapdoor.

One of the most popular public key cryptosystems is RSA, whose name is derived from Rivest-Shamir-Adleman, the algorithm's developers. The RSA algorithm was the first publickey encryption algorithm developed (in 1977) and published for commercial use. It is very popular and has been embedded in both Microsoft's and Netscape's Web browsers to enable them to provide security for e-commerce applications. The patented RSA algorithm has in fact become the de facto standard for public use encryption applications. To see how this algorithm works, see the Technical Details box "RSA Algorithm."

### 4.14.1 Technical Detail Box

**Q15. What is RSA algorithm? Explain different steps?**

*Ans :*

**RSA Algorithm**

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.

**An example of asymmetric cryptography:**

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

**The idea!** The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (*e*,*n*), the algorithm is as follows:

1. Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the *e*th power modulo n. The result is a ciphertext message C.
3. To decrypt ciphertext message C, raise it to another power d modulo n

The encryption key (*e*,*n*) is made public. The decryption key (*d*,*n*) is kept private by the user.

**How to Determine Appropriate Values for *e*, *d*, and *n***

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as *p* and *q*.
2. Set *n* equal to *p* * *q*.
3. Choose any large integer, *d*, such that GCD(*d*, ((*p*-1) * (*q*-1))) = 1
4. Find *e* such that *e* * *d* = 1 (mod ((*p*-1) * (*q*-1)))

Rivest, Shamir, and Adleman provide efficient algorithms for each required operation

**Encryption Key Size**

When using ciphers, one of the decisions that have to be made is the size of the cryptovariable or key. This will prove to be very important, because the strength of many encryption applications and cryptosystems is measured by key size. But does the size of the encryption key really matter? And how exactly does key size affect the strength of an algorithm? Typically, the length of the key increases the number of random selections that will have to be guessed in order to break the code. Creating a larger universe of possibilities that need to be checked increases the time required to make guesses, and thus a longer key will directly influence the strength of the encryption.

It may surprise you to learn that when it comes to cryptosystems, the security of encrypted data is *not* dependent on keeping the encrypting algorithm secret; in fact, algorithms should be (and often are) published, so that research to uncover their weaknesses can be done. Instead the security of any

cryptosystem depends on keeping some or all of the elements of the cryptovariable (s) or key(s) secret, and effective security is maintained by manipulating the size (bit length) of the keys and by following proper procedures and policies for key management.

For a simple example of how key size is related to encryption strength, suppose you have an algorithm that uses a three-bit key. You may recall from earlier in the chapter that keyspace is the amount of space from which the key can be drawn. Also, you may recall that in binary notation, three bits can be used to represent values from 000. to III, which correspond to the numbers 0 to 7 in decimal, and thus a keyspace of eight keys. This means that with an algorithm that uses a three-bit key you have eight possible keys to choose from (the numbers 0 to 7 in binary are 000,001,010, 011,100,101,110,111). If you know how many keys you have to choose from, you can program a computer simply to try all the keys and see if it can crack the encryptedmessage.

The preceding statement presumes a few things:

- You know the algorithm,
- You have the encrypted message, and
- You have time on your hands. It is easy to satisfy the first criterion.

The encryption tools that use the Data Encryption Standard (DES) can be purchased over the counter. Many of these tools are based on encryption algorithms that are standards, as is DES itself, therefore it is relatively easy to get a crypto system based on DES that would enable you to decrypt an encrypted message if you possess the key. The second criterion requires the interception of an encrypted message, which is illegal, but not impossible. As for the third criterion, the task required is a brute force attack, in which a computer randomly (or sequentially) selects possible keys of the known size and applies them to the encrypted text, or a piece of the encrypted text. If the result is plaintext-bingo! But as indicated earlier in this chapter, it can take quite a long time to exert brute force on the more advanced cryptosystems. In fact, the strength of an algorithm is determined by how long it takes to guess the key. Luckily, however, once set to a task, computers do not require much adult supervision, so you probably won't have to quit your dayjob.

But when it comes to keys, how big is big? From the example at the beginning of this section, you learned that a three-bit system has eight keys to guess. An eight-bit system has 256 keys to guess. Note, however, that if you use a 32-bit key, puny by modem standards, you have to guess almost 16.8 million keys. Even so, a modern PC, such as the one, could do this in mere seconds. But, as shows, the amount of time needed to crack a cipher by guessing its key grows very quickly-that is, exponentially with each additionalbit.

One thing to keep in mind here is that even though the estimated time to crack grows so rapidly with respect to the number of bits in the encryption key and the odds of cracking seem at first glance to be insurmountable, Table 8-7 doesn't account for the fact that computing power has increased (and continues to increase). Therefore, these days even the once-standard 56-bit encryption can't stand up to brute force attacks by personal computers, especially if multiple computers are used together to crack these keys. Each additional computer reduces the amount of time needed. Two computers can divide the possibilities and crack the key in approximately half the time and so on. Thus, two hundred and eighty five computers can crack a 56-bit key in one year, ten times as many would do it in a little over amonth.

**Encryption Key Power**

| It is estimated that to crack an encryption key using a brute force attack, a computer needs to perform a maximum of 2^k operations ($2^k$ guesses), where k is the number of bits in the key. In reality, the average estimated time to crack is half that time. | | | |
|---|---|---|---|
| **Using an average modern 2008-era dual-core PC performing 30,000 MIPS (million instructions per second):** | | | |
| Key Length (bits) | Maximum Number of Operations (guesses) | Maximum Time to Crack | Estimated Average Time to Crack |
| 8 | 256 | 0.0000000085 seconds | 0.0000000043 seconds |
| 16 | 65,636 | 0.0000022 seconds | 0.00000109 seconds |
| 24 | 16,777,216 | 0.00056 seconds | 0.00028 seconds |
| 32 | 4,294,967,296 | 0.143 seconds | 0.072 seconds |
| 56 | 72,057,594,037,927,900 | 27.800 days | 13.9 days |
| 64 | 18,446,744,073,709,600,000 | 19.498 years | 9.7 years |
| 128 | 3.40282E+38 | 359,676,102,360,201, 000,000 years | 179,838,051,180,100, 000,000 years |
| 256 | 1.15792E+77 | 122,391,435,436,027, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000 years | 61,195,717,718,013,400, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000 years |
| 512 | 1.3408E+154 | 14,171,960,013,891,600, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years | 7,085,980,006,945,820, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years |

**Note:** Estimated Time to crack is based on a general purpose personal computer performing eight million guesses per second

## 4.15 CRYPTOGRAPHY TOOLS PUBLIC KEY INFRASTRUCTURE

**Q16. Explain crypthographic tools to secure the information?**

*Ans :*

Public Key Infrastructure (PKI) is an integrated system of software , encryption methodologies protocols, legal agreements, and third party services that enable users to communicate security. PKI systems are based on public key cryptosystems and include digital certificates and certificate authorities (CAs)Digital certificates are public key container files that allow computer programs to validate the key and identify to who m it belongs. PKI and the digital certificate registries they contain enable the protection of information assets by making verifiable digital certificates readily available to business applications. This, in turn, allows the applications to implement several of the key characteristics of information security and to integrate these characteristics into business processes across an organization.

These processes include the following:

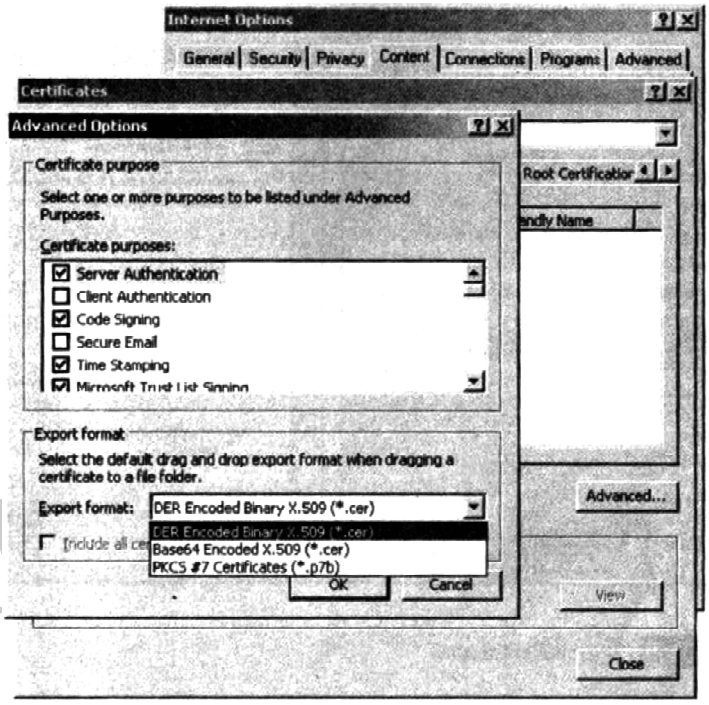
- **Authentication:** Individuals, organizations, and web servers can validate the identity of each of the parties in an internettransaction.
- **Integrity:**Contentsigned by the certificate is known to be unaltered while being moved from host to host or server to client.
- **Privacy:** Information is protected from being intercepted during transmission.

- **Authorization:** The validated identity of users and programs can be used to enable authorization rules that remain in place for the duration of a transaction; this reduces some of the overhead required and allows for more control of access privileges for specifictransactions.

  A typical PKI solution protects the transmission and reception of secure information by integrating the following components.

- A certificate authority (CA), which issues, manages, authenticates, signs, and revokes user's digital certificates, which typically contain the user's name,public key, and other identifyinginformation.

- A registration authority (RA), which operates under the trusted collaboration of the certificate authority and can be delegated day-to-day certification functions, such as verifying registration information about new registrants, generating end-user keys, revoking certificates, and validating that users possess a valid certificate.




Managing Digital Signatures

- Certificate directories, which are central locations for certificate storage that providea single access point for administration and distribution.
- Management protocols, which organize and manage the communications between CAs, RAs, and end users. This includes the functions and procedures for setting up new users, issuing keys, recovering keys, updating keys, revoking keys, and enabling the transfer of certificates and status information among the parties involved in the PKI's area of authority.
- Policiesand procedures that assistan organization in the application and mana-gement of certificates, the formalization of legal liabilities and limitations, and actual business practice use.

  Common implementations of PKI include: systems to issue digital certificates to users and servers; directory enrollment; key issuing systems; tools for managing the key and verification and return of certificates. These systems enable organizations to apply an enterprise-wide solution that provides users within the PKI's area of authority the means to implement authenticated and secure communications andtransactions.

### 4.15.1 Digital signatures

Digital signatures were created in response to the rising need to verify information transferred using electronic system. Currently, asymmetric encryption processes are used to create digital signatures. When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the sender's public key must be used to decrypt the message when the decryption happens successfully, it provides verification that the message was sent by the sender and cannot be refued.This process is known as non-repudiation and is the principle of cryptography that gives credence to the authentication mechanism collectively known as a digital signature. Digital signatures are, therefore, encrypted messages that can be mathematically proven to be authentic.

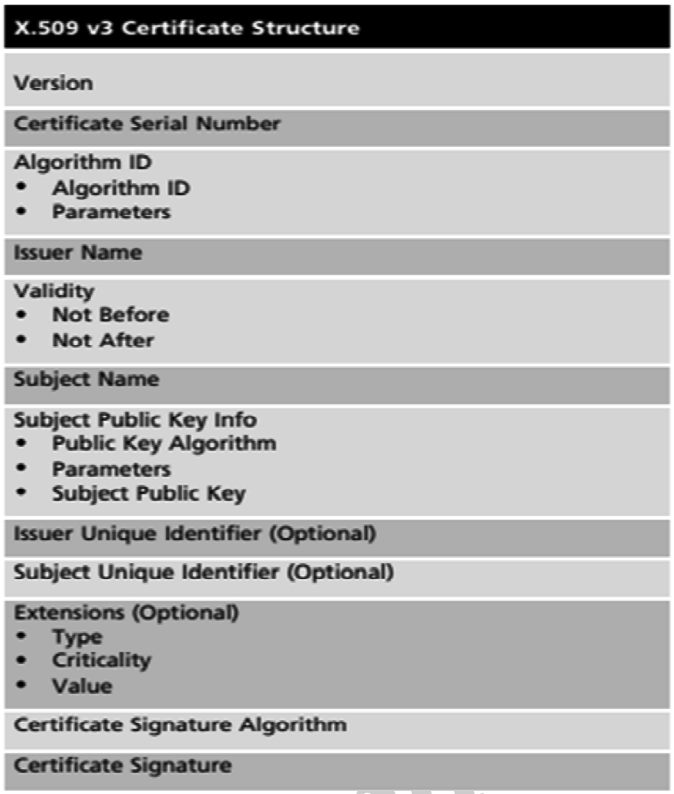
The management of digital signatures has been built into most web browsers.

**Digital Certificates**

Digital certificates are electronic documents that can be part of a process of identification associated with the presentation of a public key. Unlike digital signatures, which help authenticate the origin of a message, digital certificates authenticate the cryptographic key that is embedded in the certificate. When used properly these certificates enable diligent users to verify the authenticity of any organization's certificates. This is much like what happens when the Federal Deposit Insurance Corporation issues its "FDIC" logo to banks to help assure bank customers that their bank is authentic. Different client-server applications use different types of digital certificates to accomplish their assigned functions:

- The CA application suite issues and uses certificates that identify and establish a trust relationship with a CA to determine what additional certificates can beauthenticated.
- Mail applications use Secure/Multipurpose Internet Mail Extension (S/MIME) certificates for signing and encrypting e-mail as well as for signingforms.
- Development applications use object-signing certificates to identify signers of object- oriented code and scripts.
- Web servers and Web application servers use Secure Socket Layer (SSL) certificates to authenticate servers via the SSL protocol (which is described in anupcoming section) in order to establish an encrypted SSL session.
- Web clients use client SSL certificates to authenticate users, sign forms, and participate in single sign-on solutions viaSSL.

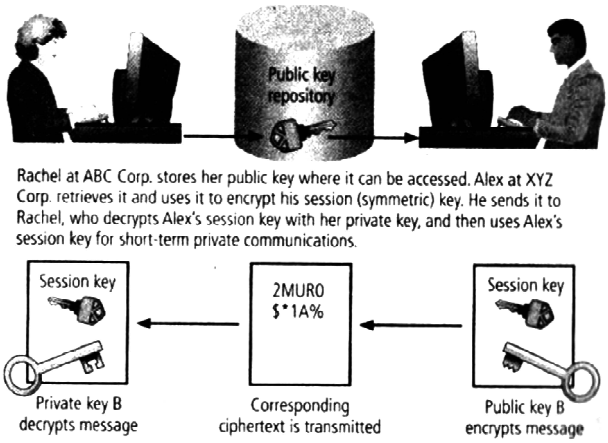
Two popular certificate types in use today are those created using Pretty Good Privacy (PGP) and those created using applications that conform to International Telecommunication Union's (ITU-T) x.509 version 3. You should know that X.S09 v3, whose structure is outlined in Table 8- 8, is an ITU-T recommendation that essentially defines a directory service that maintains a database (also known as a repository) of information about a group of users holding X.SOY v3 certificates. An X.S09 v3 certificate binds a **distinguished name (DN)**, which uniquely identifies a certificate entity, to a user's public key. The certificate is signed and placed in the directory by the CA for retrieval and verification by the user's associated public key. X.S09 v3 does not specify an encryption algorithm; however, RSA with its hashed digital signature is recommended.




### 4.15.2 Hybrid Cryptography Systems

Except in the case of digital certificates, pure asymmetric key encryption is not widely used. Asymmetric key encryption is more often used in conjunction with symmetric key encryption- thus, as part of a hybrid encryption system. The most common hybrid system is based on the **Diffie-Hellman Key Exchange method**, which is a method for exchanging private keys using public key encryption. With Diffie-Hellman, asymmetric encryption is used to exchange session keys. These are limited-use symmetric keys for temporary communications; they allow two organizations to conduct quick, efficient, secure communications based on symmetric encryption. Diffie-Hellman provided the foundation for subsequent developments in public key encryption. Because symmetric encryption is more efficient than asymmetric for sending messages, and asymmetric encryption doesn't require out-of-band key exchange, asymmetric encryption can be used to transmit symmetric keys in a hybrid approach. Diffie-Hellman avoids the exposure of data to third parties that is sometimes associated with out-of-band key exchanges.

Alex at XYZ Corp. wants to communicate with Rachel at ABC Corp., so Alex first creates a session key. Alex encrypts a message with this session key, and then gets Rachel's public key. Alex uses Rachel's public key to encrypt both the session key and the message, which is already encrypted. Alex transmits the entire package to Rachel, who uses her private key to decrypt the package containing the session key and the encrypted message, and then uses the session key to decrypt the message. Rachel can then continue to use only this session key for electronic communications until the session key expires. The asymmetric session key is used in the much more efficient asymmetric encryption and decryption processes. After the session key expires (usually in just a few minutes) a new session key will be chosen and shared using the same process.




**Example of Hybrid Encryption**

### 4.15.3 Steganography

Steganography is a process of hiding information and has been in use for a long time. In fact the word "steganography" is derived from the Greek words *steganos*meaning "covered" and *grapheinm*eaning "to write." The Greek historian Herodotus reported on one of the first steganographerswhen he described a fellow Greek sending a message to warn of an imminent invasion by writing it on the wood beneath a wax writing tablet. If the tablet were intercepted, it would appear blank. While steganography is technically not a form of cryptography, it is related to cryptography in that it also a way of transmitting information so that the information is not revealed wl1i1e it's in transit. The most popular modem version of steganography involves hiding information within files that appear to contain digital pictures or otherimages.

To understand how modern steganography works in this specific case, you must first understand a little about how images are stored. Most computer graphics standards use a combination of three color values (red, blue, and green (RGB)) to represent a picture element, or pixel. Each of the three color values usually requires an 8-bit *code* for that color's intensity (e.g., 00000000 for no red and 11111111 for maximum red). Each color pixel of an image requires 24 bits to represent the color mix and intensity. Some image encoding standards use more or fewer bits per pixel, but for the purposes of this discussion, 24-bit color will suffice. When a picture is created (by a digital camera or a computer program), the number of horizontal and vertical pixels captured and recorded is known as the image's *resolution.* Thus, for example, if 1024 horizontal pixels are recorded and 768 vertical pixels are captured, the image has a I024x768 resolution and would commonly be said to have 786,432 pixels or three-quarters of a *megapixel.* Thus, an image that is I024x768 pixels contains 786,432 groups of 24 bits to represent the red, green, and blue data. The raw image size can be calculated as 1024x768x24, or 5.66 megabytes. There are plenty of bits in this picture data file in which to hide a secret message.

To the naked eye, there is no discernible difference between a pixel with a red intensity of 00101001 and another slightly different pixel with a red intensity level of 00101000. In other words, the two different values will result in pixels that do have a discernible difference. This inability to perceive difference on part of humans provides the steganographer with one bit percolor (or three bits per pixel) to use for encoding data into an image file. If a steganographic process uses three bits per pixel for all 786,432 pixels, it will be able to store 236 kilobytes of hidden data within the uncompressed image. Some steganographic tools can calculate the maximum size image that can be stored before being detectable. In addition to digital photos, messages can be hidden in any computer file that does not utilize all of its available bits. Some applications are capable of hiding messages in .bmp, .wav, .mp3, and .au files, as well as in unused storage space on CDs and DVDs. One program can take a text or document file and hide a message in the unused whitespace.

After the attacks of September II, 200 I, U.S. federal agencies were worried that terrorist organizations were "hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards, and other websites" through the use of steganographic methods. No documented proof of this activity was ever publicized.

## 4.16 Attacks on Cryptosystems

**Q17. What is attack protocal? Explain different types attacks?**

*Ans :*

Historically, attempts to gain unauthorized access to secure communications have used brute force attacks in which the ciphertext is repeatedly searched for clues that can lead to the algorithm's structure. These attacks are known as ciphertext attacks, and involve a hacker searching for a common text structure, wording, or syntax in the encrypted message that can enable him or her to calculate the number of each type of letter used in the message. This process, known as frequency analysis, can be used along with published frequency of occurrence patterns of various languages and can allow an experienced attacker to crack almost any code quickly if the individual has a large enough sample of the encoded text. To protect against this, modern algorithms attempt to remove the repetitive and predictable sequences of characters from theciphertext.

Occasionally, an attacker may obtain duplicate texts, one in ciphertext and one in plaintext, which enable the individual to reverse-engineer the encryption algorithm in a known-plaintext attack scheme. Alternatively, attackers may conduct a selected- plaintext attack by sending potential victims a specific text that they are sure the victims will forward on to others. When the victim does encrypt and forward the message, it can be used in the attack if the attacker can acquire the outgoing encrypted version. At the very least, reverse engineering can usually lead the attacker to discover the cryptosystem that is being employed.

Most publicly available encryption methods are generally released to the information and computer security communities for testing of the encryption algorithm's resistance to cracking. In addition, attackers are kept informed of which methods of attack have failed. Although the purpose of sharing this information is to develop a more secure algorithm, it has the danger of keeping attackers from wasting their time—that is, freeing them up to find new weaknesses in the cryptosystem or new, more challenging means of obtaining encryption keys.

In general, attacks on cryptosystems fall into four general categories: man-in-the-middle, correlation, dictionary, and timing. Although many of these attacks are reiterated here in the context of cryptosystems and their impact on these systems.

### Man-in-the-Middle Attack

A man-in-the-middle attack, as discussed in Chapter 2, is designed to intercept the transmission of a public key or even to insert a known key structure in place of the requested public key. Thus, attackers attempt to place themselves between the sender and receiver, and once they've intercepted the request for key exchanges, they send each participant a valid public key, which is known only to them. From the perspective of the victims of such attacks, their encrypted communication appears to beoccurring normally, but infact the attackeris receiving each encrypted message and decoding it (with the key given to the sending party), and then encrypting and sending it to the originally intended recipient. Establishment of public keys with digital signatures can prevent the traditional man-in-the-middle attack, as the attacker cannot duplicate the signatures.

### Correlation Attacks

As the complexities of encryption methods have increased, so too have the tools and methods of cryptanalysts in their attempts to attack cryptosystems. Correlation attacks are a collection of brute-force methods that attempt to deduce statistical relationships between the structure of the unknown key and the ciphertext that is the output of the cryptosystem. Differential and linear cryptanalysis, both of which are advanced methods of breaking codes that are beyond the scope of this discussion, have been used to mount successful

attacks on block cipher encryptions such as DES. If these advanced approaches can calculate the value of the public key, and if this can be achieved in a reasonable time, all messages written with that key can be decrypted. The only defense against this kind of attack is the selection of strong cryptosystems that have stood the test of time, thorough key management, and strict adherence to the best practices of cryptography in the frequency of changing keys.

### Dictionary Attacks

In a **dictionary attack**, the attacker encrypts every word in a dictionary using the same cryptosystem as used by the target. The attacker does this in an attempt to locate a match between the target ciphertext and the list of encrypted words from the same cryptosystem. Dictionary attacks can be successful when the ciphertext consists of relatively few characters, as for example files which contain encrypted usernames and passwords. If an attacker acquires a system password file, the individual can run hundreds of thousands of potential passwords from the dictionary he or she has prepared against the stolen list. Most computer systems use a well- known one-way hash function to store passwords in such files, but this can almost always allow the attacker to find at least a few matches in any stolen password file. After a match is located, the attacker has essentially identified a potential valid password for the system underattack.

### Timing Attacks

In a timing attack, the attacker eavesdrops during the victim's session and uses statisticalanalysis of the user's typing patterns and inter-keystroke timings to discern sensitive session information. While timing analysis may not directly result in the decryption of sensitive data, it can be used to gain information about the encryption key and perhaps the cryptosystem in use. It may also eliminate' some algorithms as possible candidates, thus narrowing the attacker's search. In this narrower field of options, the attacker can increase the odds of eventual success. Once the attacker has successfully broken an encryption, he or she may launch a replay attack, which is an attempt to resubmit a recording of the deciphered authentication to gain entry into a securesource.

### Defending From Attacks

Encryption is a very useful tool in protecting the confidentiality of information that is in storage and/or transmission. However, it is just that-another tool in the information security administrator's arsenal of weapons against threats to information security. Frequently, unenlightened individuals describe information security exclusively in terms of encryption (and possibly firewalls and antivirus software). But encryption is simply the process of hiding the true meaning of information. Over the millennia, mankind has developed dramatically moresophisticated means of hiding information from those who should not see it. No matter how sophisticated encryption and cryptosystems have become, however, they have retained the same flaw that the first systems contained thousands of years ago: If you discover the key, that is, the method used to perform the encryption, you can determine the message. Thus, key management is not so much the management of technology but rather the management of people.

Encryption can, however, protect information when it is most vulnerable-that is, when it is outside the organization's systems. Information in transit through public or leased networks is an example of information that is outside the organization's control. With loss of control can come loss of security. Encryption helps organizations secure information that must travel through public and leased networks by guarding the information against the efforts of those who sniff, spoof, and otherwise skulk around. As such, encryption is a vital piece of the security puzzle.

UNIT V

**Implementing Information Security:** Information security project management, Technical topics of implementation, Non technical aspects of implementation, Security certification and accreditation.
**Security and Personnel:** Positioning and staffing security function, Employment policies and practices, Internal control strategies. Information
**Security maintenance :** Security management models, The maintenance model, Digital forensics

## 5.1 Implementing Information Security

**Q1. Explain in detail the information security project plan?**

*Ans :*

**Introduction**

An information security project manager must realize that implementing an information security project takes time, effort, and a great deal of communication and coordination. The security systems development life cycle (SecSDLC) implementation phase and describe how to successfully execute the information security blueprint. In general, the implementation phase is accomplished by changing the configuration and operation of the organization's information systems to make them more secure. It includes changes to the following:

- Procedures (for example, through policy) People (for example, through training) Hardware (for example, through firewalls) Software (for example, through encryption) Data (for example, through classification)
- The SecSDLC involves collecting information about an organization's objectives, its technical architecture, and its information security environment. These elements are used to form the information security blueprint, which is the foundation for the protection of the confidentiality, integrity, and availability of the organization's information.
- During the implementation phase, the organization translates its blueprint for information security into a project plan.
- The project plan instructs the individuals who are executing the implementation phase. These instructions focus on the security control changes that are needed to improve the security of the hardware, software, procedures, data, and people that make up the organization's information systems. The project plan as a whole must describe how to acquire and implement the needed security controls and create a setting in which those controls achieve the desired out comes.

Before developing a project plan, however, management should coordinate the organization's information security vision and objectives with the communities of interest involved in the execution of the plan. This type of coordination ensures that only controls that add value to the organization's information security program are incorporated into the project plan. If a statement of the vision and objectives for the organization's security program does notexist, one must be developed and incorporated into the project plan.

The vision statement should be concise. It should state the mission of the information security program and its objectives. In other words, the project plan is built upon the vision statement, which serves as a compass for guiding the changes necessary for the implementation phase. The components of the project plan should never conflict with the organization's vision andobjectives.

**Information Security Project Management**

As the opening vignette of this chapter illustrates, organizational change is not easily accomplished. The issues a project plan must

address, including project leadership; managerial, technical, and budgetary considerations; and organizational resistanceto thechange.

The major steps in executing the project plan are as follows: Planning the project

- Supervising tasks and action steps
- Wrapping up
- The project plan can be developed in any number of ways.

Each organization has to determine its own project management methodology for IT and information security projects. Whenever possible, information security projects should follow the organization's project management practices.

**Developing the ProjectPlan**

Planning for the implementation phase requires the creation of a detailed project plan. The task of creating such a project plan is often assigned to either a project manager or the projectchampion. This individual manages the project and delegates parts of it to other decision makers. Often the project manager is from the IT community of interest, because most other employees lack the requisite information security background and the appropriate manage ment authority and/or technical knowledge.

The project plan can be created using a simple planning tool such as the work breakdown structure (WBS).The major project tasks are placed in to the WBS, along with the following attributes for each:

- Work to be accomplished (activities and deliverables) Individuals (or skill set) assigned to perform the task Start and end dates for the task (when known)
- Amount of effort required for completion in hours or work days Estimated capital expenses for the task
- Estimated noncapital expenses for the task Identification of dependencies between and amongtasks
- Each major task on the WBS is then further divided into either smaller tasks (subtasks) or specific action steps.

For the sake of simplicity, thesample project plan isdivides each major task into action steps. Be aware that in an actual project plan, major tasks are often much more complex and must be divided into subtasks before action steps can be identified and assigned to the individual or skill set. Given the variety of possible projects, there are few formal guidelinesfor deciding what level of detail—that is, at which level a task or subtask should become an action step—is appropriate. There is, however, one hard-and-fast rule you can use to make this determination: a task or subtask becomes an action step when it can be completed by one individual or skill set and has a single deliverable.

The WBS can be prepared with a simple desktop PC spreadsheet program. The use of more complex project management software tools often leads to projectitis, wherein the project manager spends more time documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts than in accomplishing meaningful project work. Recall Kelvin's handouts from the opening vignette, which were loaded with dates and details. Kelvin's case of projectitisled him to develop an elegant, detailed plan before gaining consensus for the required changes; new to project management, he did not realize that simpler software tools would help him focus on organizing and coordinating with the project team.

- **Work to Be Accomplished** The work to be accomplished encompasses both activities and deliverables. A deliverable is a completed document or program module that can either serve as the beginning point for a later task or become an element in the finished project. Ideally, the project planner provides a label and thorough description for the task. The description should be complete enough to avoid ambiguity during the later tracking process, yet not so detailed as to make the WBS unwieldy. For instance, if the task is to write firewall specifications for the preparation of a request for proposal (RFP), the planner should note that the deliverable is a specification document suitable for distribution tovendors.

- **Assignees** The project planner should describe the skill set or person, often called a resource, needed to accomplish the task. The naming of individuals should be avoided in the early planning efforts, a rule Kelvin ignored when he named individuals for every task in the first draft of his project plan. Instead of assigning individuals, the project plan should focus on organizational roles or known skill sets. For example, if any of the engineers in the networks group can write the specifications for a router, the assigned resource would be noted as "network engineer" on the WBS. As planning progresses, however, the specific tasks and action steps can and should be assigned to individuals.
- **Start and End Dates** In the early stages of planning, the project planner should attempt to specify completion dates only for major project milestones. A milestone is a specificpoint in the project plan when a task that has a noticeable impact on the progress of the project plan is complete.
- **Amount of Effort** Planners need to estimate the effort required to complete each task, subtask, or action step. Estimating effort hours for technical work is a complex process. Even when a nor ganization has formal governance, technical review processes, and change control procedures, it is always good practice to ask the people who are most familiar with the tasks or with similar tasks to make these estimates. After these estimates are made, all those assigned to action steps should review the estimated effort hours, understand the tasks, and agree with the estimates. Had Kelvin collaborated with his peers more effectively and adopted a more flexible planning approach, much of the resistance he encountered in the meeting would not haveemerged.
- **Estimated Capital Expenses** Planners need to estimate the capital expenses required for the completion of each task, subtask, or action item. While each organization budgets and expends capital according to its own established procedures, most differentiate between capital outlays for durable assets and expenses for other purposes.
- **Estimated Noncapital Expenses** Planners need to estimate the noncapital expenses for the completion of each task, subtask, or action item. Some organizations require that this cost include a recovery charge for staff time, while others exclude employee time and onlyproject contract or consulting time as a noncapital expense. As mentioned earlier, it is important to determine the practices of the organization for which the plan is to be used.
- **Task Dependencies** Planners should note wherever possible the dependencies of other tasks or action steps on the task or action step at hand. Tasks or action steps that come before the specific task at hand are called predecessors, and those that come after the task at hand are called successors. There can be more than one type of dependency, but such details are typically covered in courses on project management and are beyond the scope of thistext.
- A sample project plan is provided below to help you better understand the process of creat- ing one. In this example, a small information security project has been assigned to Jane Smith for planning. The project is to design and implement a firewall for a single small office. The hardware is a standard organizational product and will be installed at a location that already has a network connection.

Jane's first step is to list the major tasks:

1. Contact field office and confirmnet work as sumptions.
2. Purchase standard firewallhardware.
3. Configurefirewall.
4. Package and ship firewall to fieldoffice.
5. Work with local technical resource to install and test firewall.
6. Coordinate vulnerability assessment by penetration test team.

Get remote office sign-off and update all network drawings and documentation.

| Task or Subtask | | Resources | Start and End Dates | Estimated Effort in Hours | Estimated Capital Expense | Estimated Noncapital Expense | Dependencies |
|---|---|---|---|---|---|---|---|
| 1 | Contact field office and confirm network assumptions | Network architect | S: 9/22<br>E: - | 2 | 0 | 200 | |
| 2 | Purchase standard firewall hardware | Network architect and purchasing group | S: -<br>E: - | 4 | 4,500 | 250 | 1 |
| 3 | Configure firewall | Network architect | S: -<br>E: - | 8 | 0 | 800 | 2 |
| 4 | Package and ship to field office | Student intern | S: -<br>E: 10/15 | 2 | 0 | 85 | 3 |
| 5 | Work with local technical resource to install and test firewall | Network architect | S: -<br>E: - | 6 | 0 | 600 | 4 |
| 6 | Complete vulnerability assessment by penetration test team | Network architect and penetration test team | S:<br>E: | 12 | 0 | 1,200 | 5 |
| 7 | Get remote office sign-off and update all network drawings and documentation | Network architect | S:<br>E: 11/30 | 8 | 0 | 800 | 6 |

After all the people involved review and refine Jane's plan, she revises it to add more dates to the tasks listed. Note that this version of the project plan has been further developed.

### Project Planning Considerations

As the project plan is developed, adding detail is not always straight forward. The following sections discuss factors that project planners must consider as they decide what to include in the work plan, how to break tasks into subtasks and action steps, and how to accomplish the objectives of the project.

Financial Considerations Regardless of an organization's information security needs, the amount of effort that can be expended depends on the available funds. A cost benefit analysis (CBA), typically prepared in the analysis phase of the SecSDLC, must be reviewed and verified prior to the development of the project plan. The CBA determines the impact that a specific technology or approach can have on the organization's information assets and what it may cost.

Each organization has its own approach to the creation and management of budgets and expenses. In many organizations, the information security budget is a subsection of the over- all IT budget. Public organizations tend to be more predictable in their budget processes than private organizations, because the budgets of public organizations are usually the product of legislation or public meetings. This makes it difficult to obtain additional funds once the budget is determined. Also, some public organizations rely

on temporary or renewable grants for their budgets and must stipulate their planned expenditures when the grant applications are written.

Private (for-profit) organizations have budgetary constraints that are determined by the mar- ketplace. When a for-profit organization initiates a project to improve security, the funding comes from the company's capital and expense budgets. Each for-profit organization deter- mines its capital budget and the rules for managing capital spending and expenses differ- ently. In almost all cases, however, budgetary constraints affect the planning and actual expenditures for information security. For example, a preferred technology or solution may be sacrificed for a less desirable but more affordable solution.

To justify the amount budgeted for a security project at either a public or for-profit organization, it may be useful to benchmark expenses of similar organizations.

- **Priority Considerations** In general, the most important information security controls in the project plan should be scheduled first. Budgetary constraints may have an effect on the assignment of a project's priorities.
- **Time and Scheduling Considerations** Time and scheduling can affect a project plan at dozens of points—consider the time between ordering and receiving a security control, which may not be immediately available; the time it takes to install and configure the control; the time it takes to train the users; and the time it takes to realize the return on the investment in the control.
- **Staffing Considerations** The need for qualified, trained, and available personnel also constrains the project plan. An experienced staff is often needed to implement technologies and to develop and implement policies and training programs. If no staff members are trained to configureane wfire wall, the appropriate personnel must be trained or hired.
- **Procurement Considerations** There are often constraints on the equipment and services selection processes
- **Training and Indoctrination Considera- tions** The size of theorganizationand the normal conduct of business may preclude a single large training program on new security procedures or technologies. If so, the organization should conduct a phased-in or pilot implementation, such as roll-out training for one department at a time. When a project involves a change in policies, it may be sufficient to brief supervisors on the new policy and assign them the task of updating end users in regularly scheduled meetings. Project planners must ensure that compliance documents are also distributed and that all employees are required to read, understand, and agree to the newpolicies.

**Scope Considerations**

- **Project scope** describes the amount of time and effort-hours needed to deliver the planned features and quality level of the project deliverables. The scope of any given project plan should be carefully reviewed and kept as small as possible given the project's objectives.
- There are several reasons why the scope of information security projects must be evaluated and adjusted with care. First, in addition to the challenge of handling many complex tasks at one time, the installation of information security controls can disrupt the ongoing opera- tions of an organization, and may also conflict with existing controls in unpredictable ways. For example, if you install a new packet filtering router and a new application proxy firewall at the same time and, as a result, users are blocked from accessing the Web, which technol- ogycaused the conflict? Was it the router, the firewall, or an interaction between the two? Limiting the project scope to a set of manageable tasks does not mean that the project should only allow change to one component at a time, but a good plan carefully considers the num- ber of tasks that are planned for the same time in a singledepartment.
- Recall from the opening vignette that all of Kelvin's change requests are in the area

ofnetwork- ing, where the dependencies are particularly complex. If the changes in Kelvin's project plan are not deployed exactly as planned, or if unanticipated complexities arise, there could be extensive disruption to Sequential Label and Supply's daily operations. For instance, an error in the deployment of the primary firewall rules could interrupt all Internet connectivity, which might, inturn,make the early detection of (and recovery from) the original error more difficult.

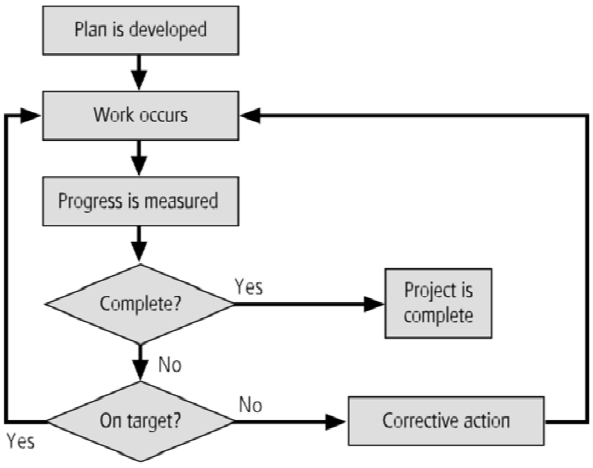
### 5.1.1 The Need for Project Management

**Q2. Explain the need of project plan?**

*Ans :*

Project management requires a unique set of skills and a thorough understanding of a broad body of specialized knowledge. In the opening vignette, Kelvin's inexperience as a project manager makes this all too clear. Realistically, most information security projects require a trained project manager—a CISO or a skilled IT manager who is trained in project manage- ment techniques. Even experienced project managers are advised to seek expert assistance when engaging in a formal bidding process to select advanced or integrated technologies or outsourced services.

- **Supervised Implementation** Although it is not an optimal solution, some organizations designate a champion from the general management community of interest to supervise the implementation of an information security project plan. In this case, groups of tasks are delegated to individuals or teams from the IT and information security communities of interest. An alternative is to designate a senior IT manager or the CIO of the organization to lead the implementation. In this case, the detailed work is delegated to cross-functional teams.The optimal solution is to designate a suitable person from the information security community of interest. In the final analysis, each organization must find the project leadership that best suits its specific needs and the personalities and politics of the organizational culture.
- **Executing the Plan** Once a project is underway, it is managed using a process known as a **negative feedback loop** or cybernetic loop, which ensures that progress is measured periodically. In the negative feedback loop, measured results are compared to expected results. When significant deviation occurs, corrective action is taken to bring the deviating task back into compliance with the project plan, or else the projection is revised in light of newinformation.
- **Corrective action is taken in two basic situations:** either the estimate was flawed, or perfor- mance has lagged. When an estimate is flawed, as when the number of effort-hours required is underestimated, the plan should be corrected and downstream tasks updated to reflect the change. When performance has lagged, due, for example, to high turnover of skilled employees, corrective action may take the form of adding resources, making longer sche- dules, or reducing the quality or quantity of the deliverable. Corrective action decisions are usually expressed in terms of trade-offs. Often a project manager can adjust one of the three following planning parameters for the task being corrected:
  - Effort and money allocated Elapsed time or
  - schedulingimpact
  - Quality or quantity of the deliverable




- When too much effort and money is being spent, you may decide to take more time to com- plete the project tasks or to lower the deliverable quality or quantity. If the task is taking too long to complete, you should probably add more resources in staff time or money or else lower deliverable quality or quantity. If the quality of the deliverable is too low, you must usually add more resources in staff time or money or take longer to complete the task. Of course, there are complex dynamics among these variables, and these simplistic solutions do not serve in all cases, but this simple trade-off model can help the project man- ager to analyze availableoptions.
- **Project Wrap-up Projectwrap-up** is usually handled as a procedural task and assigned to a mid-level IT or information security manager. These managers collect documentation, finalize status reports, and deliver a final report and a presentation at a wrap-up meeting. The goal of the wrap-up is to resolve any pending issues, critique the overall project effort, anddrawconclusionsabouthowtoimprovetheprocessforthefuture.

## 5.2 Technical Aspects of Implementation

**Q3. Discuss technical issues related to project plan management?**

*Ans :*

The implementation process are technical in nature and deal with the application of technology, while others deal instead with the human interface to technical systems.

**Conversion Strategies**

As the components of the new security system are planned, provisions must be made for the changeover from the previous method of performing a task to the new method. Just like IT systems, information security projects require careful conversion planning. In both cases, four basic approaches used for changing from an old system or process to a new one are:

- **Direct changeover:** Also known as going "cold turkey," a direct changeover involves stopping the old method and beginning the new. This could be as simple as having employees follow the existing procedure one week and then use a new procedure the next. Some cases of direct changeover are simple, such as requiring employees to use a new password (which uses a stronger degree of authentication) beginning on an announced date; some may be more complex, such as requiring the entire company to change procedures when the network team disables an old firewall and activates a new one. The primary drawback to the direct changeover approach is that if the new system fails or needs modification, users may be without services while the system's bugs are worked

out. Complete testing of the new system in advance of the direct change- over reduces the probability of such problems.

- **Phased implementation:**A **phased implementation** is the most common conversion strategy and involves a measured rollout of the planned system, with a part of the whole being brought out and disseminated across an organization before the next piece is implemented. This could mean that the security group implements only a small portion of the new security profile, giving users a chance to get used to it and resolving issues as they arise. This is usually the best approach to security project implementation. For example, if an organization seeks to update both its VPN and IDPS systems, it may first introduce the new VPN solution that employees can use to connect to the organization's network while they're traveling. Each week another department will be allowed to use the new VPN, with this process continuing until all departments are using the new approach. Once the new VPN has been phased into operation, revisions to the organization's IDPS can begin.
- **Pilot implementation:** In a **pilot implementation**, the entire security system is put in place in a single office, department, or division, and issues that arise are dealt with before expanding to the rest of the organization. The pilot implementation works well when an isolated group can serve as the "guinea pig," which prevents any problems with the new system from dramatically interfering with the performance of the organization as a whole. The operation of a research and development group, for example, may not affect the real-time operations of the organization and could assist security in resolving issues that emerge.
- **Parallel operations:** The **parallel operations** strategy involves running the new methods alongside the old methods. In general, this means running two systems concurrently; in terms of information systems, it might involve, for example, running two firewalls concurrently. Although this approach is complex, it can reinforce an organization's information security by allowing the old system(s) to serve as backup for the new systems if they fail or are compromised. Drawbacks usually include the need to deal with both systems and maintain both sets of procedures.

### 5.2.1 The Bull's-eye Model

**Q4. Explain in detail the Bull's-eye model in solving systematic & measure way of information security?**

*Ans :*

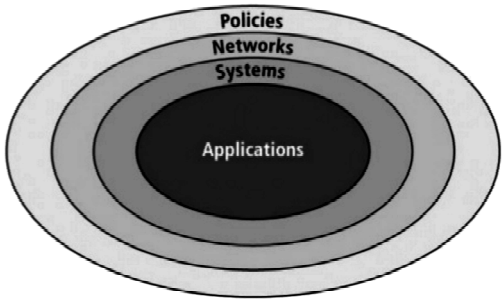
A proven method for prioritizing a program of complex change is the bull's-eye method. This methodology, which goes by many different names and has been used by many organizations, requires that issues be addressed from the general to the specific, and that the focus be on systematic solutions instead of individual problems. The increased capabilities—that is, increased expenditures—are used to improve the information security program in a systematic and measured way. the approach relies on a process of project plan evaluation in four layers:

1. **Policies:** This is the outer, or first, ring in the bull's-eye diagram. The critical importance of policies has been emphasized throughout. The foundation of all effective information security programs is sound information security and information technology policy. Since policy establishes the ground rules for the use of all systems and describes what is appropriate and what is inappropriate, it enables all other information security components to function correctly. When deciding how to implement complex changes and choose from conflicting options, you can use policy to clarify what the organization is trying to accomplish with itsefforts.
2. **Networks:** In the past, most information security efforts focused on this layer, and so until recently information security was often considered synonymous with network security. In today's computing environment, implementing information security is more

complex because networking infrastructure often comes into contact with threats from the public network. Those organizations new to the Internet find (as soon as their policy environment defines how their networks should be defended) that designing and implementing an effective DMZ is the primary way to secure an organization's networks. Secondary efforts in this layer include providing the necessary authentication and authorization when allowing users to connect over public networks to the organization's systems.

3. **Systems:** Many organizations find that the problems of configuring and operating information systems in a secure fashion become more difficult as the number and complexity of these systems grow. This layer includes computers used as servers, desktop computers, and systems used for process control and manufacturing systems.

4. **Applications:** The layer that receives attention last is the one that deals with the application software systems used by the organization to accomplish its work. This includes packaged applications, such as office automation and e-mail programs, as well as high- end enterprise resource planning (ERP) packages than span the organization. Custom application software developed by the organization for its own needs is also included.




By reviewing the information security blueprint and the current state of the organization's information security efforts in terms of these four layers, project planners can determine which areas require expanded information security capabilities. The bull's-eye model can also be used to evaluate the sequence of steps taken to integrate parts of the information security blueprint into a project plan. As suggested by its bull's-eye shape, this model dictates thefollowing:

- Until sound and useable IT and information security policies are developed, communicated, and enforced, no additional resources should be spent on other controls.
- Until effective network controls are designed and deployed, all resources should go toward achieving this goal (unless resources are needed to revisit the policy needs of the organization).
- After policies and network controls are implemented, implementation should focus on the information, process, and manufacturing systems of the organization. Until there is well-informed assurance that all critical systems are being configured and operated in a secure fashion, all resources should be spent on reaching that goal.

Once there is assurance that policies are in place, networks are secure, and systems are safe, attention should move to the assessment and remediation of the security of the organization's applications. This is a complicated and vast area of concern for many organizations. Most organizations neglect to analyze the impact of information security on existing purchased and their own proprietary systems. As in all planning efforts, attention should be paid to the most critical applications first.

**To Outsource orNot**

Not every organization needs to develop an information security department or program of its own. Just as some organizations outsource part of or all of their IT operations, so too can organizations

outsource part of or all of their information security programs. The expense and time required to develop an effective information security program may be beyond the means of some organizations, and therefore it may be in their best interest to hire professional services to help their IT department simplement such a program.

When an organization outsources most or all IT services, information security should be part of the contract arrangement with the supplier. Organizations that handle most of their own IT functions may choose to outsource the more specialized information security functions. Small and medium-sized organizations often hire outside consultants for penetration testing and information security program audits. Organizations of all sizes frequently outsource net- work monitoring functions to make certain that their systems are adequately secured and to gain assistance in watching for attempted or successful attacks.

**Technology Governance and ChangeControl**

Other factors that determine the success of an organization's IT and information security programs are technology governance and change control processes.

**Technology governance**, a complex process that organizations use to manage the effects and costs of technology implementation, innovation, and obsolescence, guides how frequently technical systems are updated and how technical updates are approved and funded. Technology governance also facilitates communication about technical advances and issues across the organization.

Medium and large-sized organizations deal with the impact of technical change on the operation of the organization through a change control process. By managing the process of change, the organization can do thefollowing:

- Improve communication about change across the organization
- Enhance coordination between groups within the organization as change is scheduled and completed
- Reduce unintended consequences by having a process to resolve conflict and disruption that change can introduce
- Improve quality of service as potential failures are eliminated and groups work together
- Assure management that all groups are complying with the organization's policies regarding technology governance, procurement, accounting, and information security
- Effective change control is an essential part of the IT operation in all but the smallest organizations. The information security group can also use the change control process to ensure that the essential process steps that assure confidentiality, integrity, and availability are fol- lowed when systems are upgraded acrossthe organization.

## 5.3 NONTECHNICAL ASPECTS OF IMPLEMENTATION

**Q5. Explain the culture of change manage- ment for organization changes?**

*Ans :*

Some aspects of the information security implementation process are not technical in nature, and deal instead with the human interfaceto technical systems. In the sections that follow, the topic of creating a culture of change management and the considerations for organizations facing change are discussed.

**The Culture of ChangeManagement**

The prospect of change, the familiar shifting to the unfamiliar, can cause employees to build up, either unconsciously or consciously, a resistance to that change. Regardless of whether the changes are perceived as good (as in the case of information security implementations) or bad (such as downsizing or massive restructuring), employees tend to prefer the old way of doing things. Even when employees embrace changes, the stress of actually making the changes and adjusting to the new procedures can increase the probability of mistakes or create vulnerabil- itiesin systems. By understanding and applying some of the basic tenets of change management, project managers can lower employee resistance to change and can even build resilience to change, thereby making on going change more palatable to the entire organization.

The basic foundation of change management requires that those making the changes understand that organizationstypically have cultures that represent their mood and philosophy. Disruptions to this culture must be properly addressed and their effects minimized. One of the oldest models of change is the Lewinchange model, which consists of:

- Unfreezing
- Moving
- Refreezing

Unfreezing involves thawing hard-and-fast habits and established procedures. Moving is the transition between the old way and the new. Refreezing is the integration of the new methods into the organizational culture, which is accomplished by creating an atmosphere in which the changes are accepted as the preferred way of accomplishing the necessary tasks.

**Considerations for Organizational Change**

Steps can be taken to make an organization more amenable to change. These steps reduce resistance to change at the beginning of the planning process and encourage members of the organization to be more flexible as changes occur.

**Reducing Resistance to Change from the Start**

The level of resistance to changeaffects the ease with which an organization is able to implement procedural and managerial changes. The more ingrained the existing methods and behaviors are, the more difficult making the change is likely to be. It's best, therefore, to improve the interaction between the affected members of the organization and the project planners in the early phases of an information security improvement project. The interaction between these groups can be improved through a three-step process in which project managers communicate, educate, andinvolve.

Communication is the first and most critical step. Project managers must communicate with the employees, so that they know that a new security process is being considered and that their feedback is essential to making it work. You must also constantly update employees on the progress of the SecSDLC and provide information on the expected completion dates. This ongoing series of updates keeps the process from being a last-minute surprise and primes people to accept the change more readily when it finally arrives.

At the same time, you must update and educate employees about exactly how the proposed changes will affect them individually and within the organization. While detailed information may not be available in earlier stages of a project plan, details that can be shared with employees may emerge as the SecSDLC progresses. Education also involves teaching employees to use the new systems once they are in place. This, as discussed earlier, means delivering high-quality training programs at the appropriate times.

Finally, project managers can reduce resistance to change by involving employees in the project plan. This means getting key representatives from user groups to serve as members of the Sec SDLC development process. In systems development, this is referred to as joint application development, or JAD. Identifying a liaison between IT and information security implementers and the general population of the organization can serve the project team well in early planning stages, when unfore seen problems with acceptance of the project may need to bead dressed.

**Developing a Culturethat Supports Change**

An ideal organization fosters resilience tochange. This means the organization understands that change is a necessary part of the culture, and that embracing change is more productive than fighting it. To develop such a culture, the organization must successfully accomplish many projects that require change. A resilient culture can be either cultivated or undermined by management's approach. Strong management support for change, with a clear executive-level champion, enables the organization to recognize the necessity for and strategic importance of the change. Weak management support, with overly delegated responsibility and no champion, sentences the project to almost-certain failure. In this case, employ ees sense the low priority that has been given to the project and do not communicate with represen-tatives from the development team because the effort seemsuseless.

## 5.4 Information Systems Security Certification and Accreditation

**Q6. What are certifications that information security personnely should aquire?**

*Ans :*

It may seem that only systems handling secret government data require security certification or accreditation. However, organizations are increasingly finding that, in order to comply with the myriad of new federal regulation protecting personal privacy, their systems need to have some formal mechanism for verification and validation.

**Certification versus Accreditation**

In security management, accreditation is what authorizes an IT system to process, store, or transmit information. It is issued by a management official and serves as a means of assuring that systems are of adequate quality. It also challenges managers and technical staff to find the best methods to assure security, given technical constraints, operational constraints, and mission requirements. In the same vein, certification is "the comprehensive evaluation of the technical and nontechnical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements." Organizations pursue accreditation or certification to gain acompetitive advantage orto provide assurance to their customers. Federal systems require accreditation under OMB Circular A-130 and the Computer Security Act of 1987. Accreditation demonstrates that management has identified an acceptable risk level and provided resources to control unacceptable risk levels.

Accreditation and certification are not permanent. Just as standards of due diligence and due care require an ongoing maintenance effort, most accreditation and certification processes require reaccreditation or recertification every few years (typically every three to five years).

NISTSP800-37, Rev.1: Guide for Applying the Risk Management Framework to Federal Information Systems: ASecurity Life Cycle Approach

Two documents provide guidance for the certification and accreditation of federal information systems: SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, and CNSS Instruction-1000: National Information Assurance Certification and Accreditation Process (NIACAP).

Information processed by the federal government is grouped into one of three categories: national security information (NSI), non-NSI, and intelligence community (IC). National security information is processed on national security systems (NSSs). NSSs are managed and operated by the Committee for National Systems Security (CNSS), and non-NSSs are managed and operated by the National Institute of Standards and Technology (NIST). Intelligence community (IC) information is a separate category and is handled according to guidance from the office of the Director of NationalIntelligence (DNI).

An NSS is defined as any information system (including anytelecommunications system) used or operated by an agency or by a contractor of any agency, or other organization on behalf of anagency, the function, operation, or use of which:

- Involves intelligence activities
- Involves cryptologic activities related to national security Involves command and control of military forces
- Involves equipment that is an integral part of a weapon or weapon system
- Is subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions, or is protected at all times by procedures for information that have been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy

Subparagraph (B) states that this criterion "does not include a system that is to be used for

routine administration and business applications (including payroll, finance, logistics, and personnel management applications)".

National security information must be processed on NSSs, which have more stringent requirements. NSSs (which process a mix of NSI and non-NSI) are accredited using CNSS guidance. Non-NSS systems follow NIST guidance. More than a score of major government agencies store, process, or transmit NSI, and many of them have both NSSs and systems that are not rated as NSSs. You can learn more about the CNSS community and how NSSs are managed and operated at www.cnss.gov.

In recent years, the Joint Task Force Transformation Initiative Working Group of the U.S. government and NIST have worked to overhaul the formal certification and accreditation (C&A) program for non-NSI systems from a separate C&A process into an integrated risk management framework (RMF), which can be used for normal operations and yet still provide assurance that the systems are capable of reliably housing confidential information. Revision 1 to NIST SP 800-37 provides a detailed description of the new RMF process. The following section is adapted from this document.

The revised process emphasizes: (i) building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational opera- tions and assets, individuals, other organizations, and the Nation arising from theoperationanduseofinformationsystems.

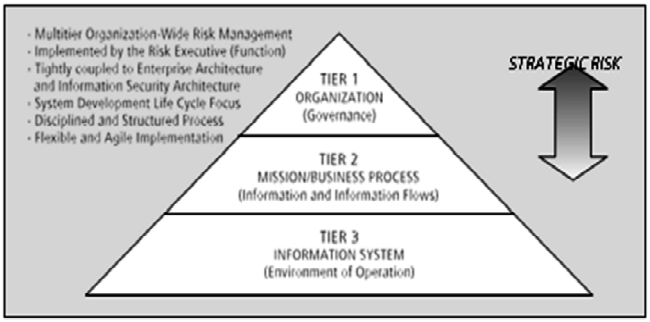
The risk management process described in this publication changes the traditional focus of C&A as a static, procedural activity to a more dynamic approach that provides the capability to more effectivelymanageinformationsystem-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions.

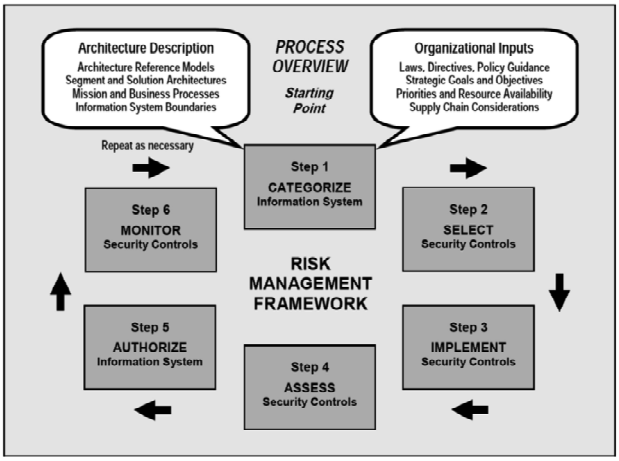
The guidelines in SP 800-37 Rev. 1 are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.

The U.S. federal government is replacing the old C&A process with a formal RMF, that framework is briefly described here. SP 800-37 Rev. 1 specifically refers to NIST SP 800-39, a new publication titled Integrated Enterprise-Wide Risk Management: Organization, Mission and Information Systems View as the reference for its RMF. The NIST RMF builds on a three-tiered approach to risk manage mentthat addresses risk-related concerns at the organization level, the mission and business process level, and the information system level, Tier 1 addresses riskfrom an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy.

Tier 2 addresses risk from a mission and business process perspective and is guided by the risk decisions at Tier 1. Tier 2 activities are closely associated with enterprise architecture

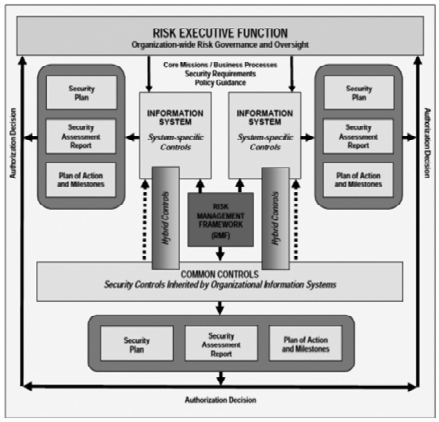
Tier 3 addresses risk from an information system perspective and is guided by the risk decisions at Tiers 1 and 2. Risk decisions at Tiers 1 and 2 impact theultimate selection and deployment of needed safeguards and countermeasures (i.e., security controls) at the information system level. Information security requirements are satisfied by the selection of appropriate management, operational, and technical security controls from NIST Special Publication800-53.




Risk management activities into the system development life cycle. The RMF operates primarily at Tier 3 in the risk management hierarchy but can also have interactions at Tiers 1 and 2 (e.g., providing feedback from ongoing authorization decisions to the risk executive [function], dissemination of updated threat and risk information to authorizing officials and information systemowners).The RMF steps include:

- Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- Select an initial set of baseline security controls for the information sys2tem based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and localconditions.
- Implement the security controls and describe how the controls are employed within the information system and its environment of operation.
- Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.




Why is it important thatyou know this information? Your organization may someday wish to become (or may already be) a government contractor, and these guidelines apply to all sys- temsthat connect to U.S. government systems not identified as national security systems or as containing national securityinformation.

**RMF Step 1—Categorize Information System**·

- **(Security Categorization) :** Categorize the information system and document the results of the security categorization in the securityplan.
- **(Information System Description) :** Describe the information system (including system boundary) and document the description in the securityplan.·
- **(Information System Registration) :** Register the information system with appropriate organizational program/ management offices.

**Milestone Checkpoint for RMF Step 1:**·

- Has the organization completed a security categorization of the information system including the information to be processed, stored, and transmitted by the system?·
- Are the results of the security categorization process for the information system consistent with the organization's enterprise architecture and commitment to protecting organizational mission/business processes?·
- Do the results of the security categorization process reflect the organization's risk management strategy? Has the organization adequately described the characteristics of the information system?· Has the organization registered the information system for purposes of management, accountability, coordination, and oversight?

**RMF Step 2—Select Security Controls**·

- **(Common Control Identification):** Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).
- **(SecurityControlSelection):** Select the security controls for the information system and document the controls in the securityplan.
- **(Monitoring Strategy):** Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.·
- **(SecurityPlanApproval):** Review and approve the security plan.

**Milestone Checkpoint for RMF Step 2:**

- Has the organization allocated all security controls to the information system as system-specific, hybrid, or common controls?
- Has the organization used its risk assessment (either formal or informal) to inform and guide the security control selection process?
- Has the organization identified authorizing officials for the information system and all common controls inherited by the system?
- Has the organization tailored and supplemented the baseline security controls to ensure that the controls, if implemented, adequately mitigate risks to organizational operations and assets, individuals, other organizations, and the nation?
- Has the organization addressed minimum assurance requirements for the security controls employed within and inherited by the information system?
- Has the organization consulted information system owners when identifying common controls to ensure that the security capability provided by the inherited controls is sufficient to deliver adequate protection?
- Hastheorganizationsupplementedthecommoncontrolswithsystem-specificorhybridcontrolswhenthe security control baselines of the common controls are less than those of the information system inheriting thecontrols?
- Has the organization documented the common controls inherited from external providers?
- Has the organization developed a continuous monitoring strategy for the information system (including monitoring of security control effectiveness for system-specific, hybrid, and common controls) that reflects the organizational risk management strategy and organizational commitment to protecting critical missions and business functions?
- Have appropriate organizational officials approved security plans containing system-specific, hybrid, and common controls?

**RMF Step 3—Implement Security Controls**

- **(Security Control Implementation):** Implement the security controls specified in the security plan.
- **(Security Control Documentation):** Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expectedoutputs).

**Milestone Checkpoint for RMF Step 3:**

- Has the organization allocated security controls as system-specific, hybrid, or common controls consistent with the enterprise architecture andinformation security architecture?
- Has the organization demonstrated the use of sound information system and security engineering methodologies in integrating information technology products into the information system and in implementing the security controls contained in the security plan?
- Has the organization documented how common controls inherited by organizational information systems have been implemented?

- Has the organization documented how system-specific and hybrid security controls have been implemented within the information system taking into account specific technologies and platform dependencies?·
- Has the organization taken into account the minimum assurance requirements when implementing security controls?

**RMF Step 4—Assess Security Controls**·

- **(AssessmentPreparation):** Develop, review, and approve a plan to assess the security controls.·
- **(Security Control Assessment):** Assess the security controls in accordance with the assessment procedures defined in the security assessmentplan.·
- **(SecurityAssessmentReport):** Prepare the security assess mentreport documenting theissues, findings, and recommendations from the security controlassessment.·
- **(Remediation Actions):** Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), asappropriate.

**Milestone Checkpoint for RMF Step 4:**·

- Has the organization developed a comprehensive plan to assess the security controls employed within or inherited by the information system?·
- Was the assessment plan reviewed and approved by appropriate organizational officials?· Has the organization considered the appropriate level of assessor independence for the security control assessment?·
- Has the organization provided all of the essential supporting assessment-related materials needed by the assessor(s) to conduct an effective security control assessment?·
- Has the organization examined opportunities for reusing assessment results from previous assessments or from other sources?·
- Did the assessor(s) complete the security control assessmentin accordance with the state dassessmentplan?
- Did the organization receive the completed security assessment report with appropriate findings and recommendations from theassessor(s)?·
- Did the organization take the necessary remediation actions to address the most important weaknesses and deficiencies in the information system and its environment of operation based on the findings and recommendations in the security assessment report?·
- Did the organization update appropriate security plans based on the findings and recommendations in the security assessment report and any subsequent changes to the information system and its environment of operation?

**RMF Step 5—Authorize Information System**·

- **(Plan of Action and Milestones):** Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.·
- **(Security Authorization Package):** Assemble the security authorization package and submit the package to the authorizing official foradjudication.·

- **(Risk Determination):** Determine the risk to organizational operations (including mission, functions, image, or reputation), organizationalassets, individuals, otherorganizations, orthenation.·
- **(Risk Acceptance):** Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the nation isacceptable.

**Milestone Checkpoint for RMF Step 5:**·

- Did the organization develop a plan of action and milestones reflecting organizational priorities for addressing the remaining weaknesses and deficiencies in the information system and its environment of operation?·
- Did the organization develop an appropriate authorization package with all key documents including the security plan, security assessment report, and plan of action and milestones (if applicable)?·
- Did the final risk determination and risk acceptance by the authorizing official reflect the risk management strategy developed by the organization and conveyed by the risk executive (function)?·
- Was the authorization decision conveyed to appropriate organizational personnel including information system owners and common control providers?

**RMF Step 6—Monitor Security Controls**·

- **(InformationSystemandEnvironmentChanges):** Determine the security impact of proposed or actual changes to the information system and its environment of operation.·
- **(OngoingSecurityControlAssessments):** Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoringstrategy.·
- **(Ongoing Remediation Actions):** Conduct remediation actions based on the results of ongoing monitoring activities,assessment of risk, and outstanding items in the plan of action and milestones.·
- **(KeyUpdates):** Update the security plan, security assessm entreport, and plan of action and mile stones based ontheresultsofthecontinuousmonitoringprocess.·
- **(SecurityStatusReporting):** Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriateorganizational officials on a non going basis in accordance with them on it oringstrategy.·
- **(Ongoing Risk Determination and Acceptance):** Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the nation remain sacceptable.·
- **(InformationSystemRemovalandDecommissioning):** Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

**Milestone Checkpoint for RMF Step 6:**

- Is the organization effectively monitoring changes to the information system and its environment of operation including the effectiveness of deployed security controls in accordance with the continuous monitoring strategy?

- Is the organization effectively analyzing the security impacts of identified changes to the information system and its environment of operation?
- Is the organization conducting ongoing assessments of security controls in accordance with the monitoring strategy?
- Is the organization taking the necessary remediation actions on an ongoing basis to address identified weaknesses and deficiencies in the information system and its environment of operation?
- Does the organization have an effective process in place to report the security status of the information system and its environment of operation to the authorizing officials and other designated senior leaders within the organization on an ongoing basis?
- Is the organization updating critical risk management documents based on ongoing monitoring activities? Are authorizing officials conducting ongoing security authorizations by employing effective continuous monitoring activities and communicating updated risk determination and acceptance decisions to information system owners and common control providers?

### 5.4.1 NSTISS Instruction-1000: National Information Assurance Certification and Accreditation Process (NIACAP)

**Q7. What are the 4 phases of NIACAP & instructions? What NIACAP certification levels are recommeded by the security levels?**

*Ans :*

National security interest systems have their own security C & Astandards, which also follow the guidance of OMB Circular A-130. The Committee on National Systems Security (CNSS) (formerly known as the National Security Telecommunications and Information Systems Security Committee or, NSTISSC) document is titled "NSTISS Instruction 1000: National Information Assurance Certification and Accreditation Process (NIACAP)"; see www.cnss. gov/Assets/pdf/nstissi-1000.pdf. The following section contain sexcerpts from this document and provides an over view of the purpose andp rocessof this certification and accreditation program.

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), establishes the minimum national standards for certifying and accrediting national security systems. This process provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site. This process focuses on an enterprise-wide view of the information system (IS) in relation to the organization's mission and the IS business case.

2. The NIACAP is designed to certify that the IS meets documented accreditation requirements and will continue to maintain the accredited security posture throughout the sys- tem lifecycle.

   The key to the NIACAP is the agreement between the IS program manager, designated approving authority (DAA), certification agent (certifier), and user representative. These individuals resolve critical schedule, budget, security, functionality, and performance issues.

The NIACAP agreements are documented in the system security authorization agreement (SSAA). The SSAA is used to guide and document the results of the C&A process. The objectiveis to use the SSAA to establish an evolving yet binding agreement on the level of security required before the system development begins or changes to a system are made. After accreditation, the SSAA becomes the baseline security configurationdocument.

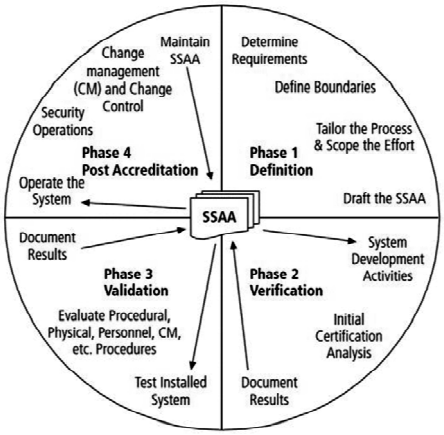
The minimum NIACAP roles include the program manager, DAA, certifier, and user representative. Additional roles may be added to increase the integrity and objectivity of C&A decisions. For example, the information systems security officer (ISSO) usually performs a key role in the maintenance of the security posture after accreditation and may also play a key role in the C&A ofthe system.

**The SSAA:**

- Describes the operating environment and threat Describes the system security architecture
- Establishes the C&A boundary of the system to be accredited
- Documents the formal agreement among the DAA(s), certifier, program manager, and user representative
- Documents all requirements necessary for accreditation
- Minimizes documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations, architecture description, test procedures, etc)
- Documents the NIACAP plan
- Documents test plans and procedures, certification results, and residual risk Forms the baseline security configuration document

The NIACAP is composed of four phases as shown from several perspectives. Thesephasesaredefinition,verification,validation,andpostaccreditation.

1. **Phase 1**, definition, determines the necessary security measures and effort level to achieve certificationand accreditation. The objective of Phase 1 is to agree on the security requirements, C&A boundary, schedule, level of effort, and resources required.
2. **Phase 2**, verification, verifies the evolving or modified system's compliance with the information in the SSAA. The objective of Phase 2 is to ensure the fully integrated system is ready for certification testing.
3. **Phase 3**, validation, validates compliance of the fully integrated system with the security policy and requirements stated in the SSAA. The objective of Phase 3 is to produce the required evidence to support the DAA in making an informed decision to grant approval to operate the system (accreditation or interim approval to operate [IATO]).




**4.** **Phase 4,** post accreditation, starts after the system has been certified and accredited for operations. Phase 4 includes those activities necessary for the continuing operation of the accredited IS and manages the changing threats and small-scale changes a system faces through its life cycle. The objective of Phase 4 is to ensure secure system management, operation, and maintenance sustainan acceptable level of residual risk.

The accreditation process itself is so complex that professional certifiers must be trained. The CNSS has a set of training standards for federal information technology workers who deal with information security. One of these documents, NSTISSI 4015, provides a national training standard for systems certifiers.

A qualified systems certifier must be formally trained in the fundamentals of INFOSEC and have field experience. It is recommended that system certifiers have system administrator and/or basic information system security officer (ISSO) experience, and be familiar with the knowledge, skills, and abilities required of the DAA, as illustrated in NSTISSI 4015. Once this professional completes training based on NSTISSI-4015, which includes material from NSTISSI-1000, they are eligible to be a federal agency systems certifier.

### 5.4.2 ISO 27001/27002 Systems Certification and Accreditation

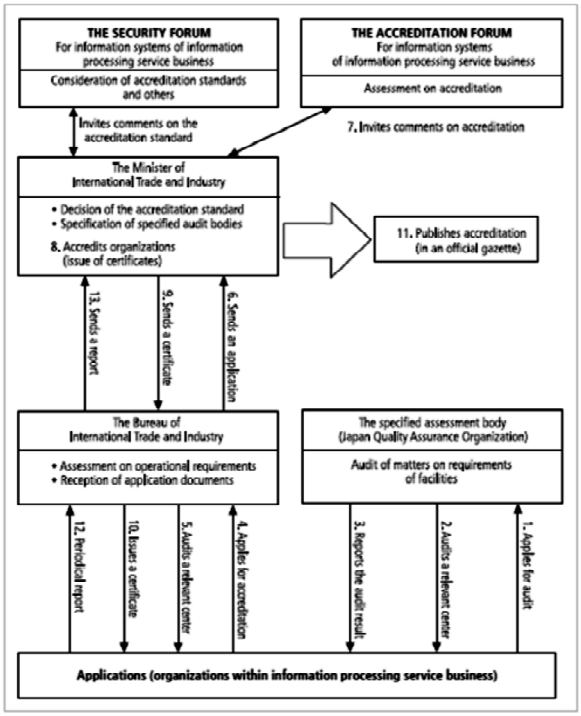
**Q8. What is 27001/27002? What are the benefits of ISO 27001/27002? What is the cost of cetification?**

*Ans :*

Entities outside the United States apply the standards provided under the International Standards Organization standard ISO 27001 and 27002, Recall that the standards were originally created to provide a foundation for British certification of information security management systems (ISMS). Organizations wishing to demonstrate their systems have met this international standard must follow the certification process, which includesthe followingphases:

- The first phase of the process involves your company preparing and gettingready for the certification of your ISMS: developing and implementing your ISMS, using and integrating your ISMS into your day to day business processes, train- ingyourstaffandestablishinganon-going program of ISMS maintenance.

- The second phase involves employing one of the accredited certification bodies to carry out an audit of your ISMS.
- The certificate that is awarded will last for three years after which the ISMS needs to be recertified. Therefore there is a third phase of the process (assuming the certification has been successful and a certificate has been issued), which involves the certification body visiting your ISMS site on a regular basis (e.g. every 6–9 months) to carry out a surveillance audit.




## 5.5 SECURITY AND PERSONNEL

**Q9. What are the qualities & goals of information security with in an organization?**

*Ans :*

**Introduction**

When implementing information security, an organization must address various issues. First, it must decide how to position and name the security function. Second, the information security community of interest must plan for the proper staffing (or adjustments to the staffing plan) for the information security function. Third, the IT community of interest must assess the impactof information security on every IT function and adjust job descriptionsand documented practices accordingly.

In order to assess the effect that the changes will have on the organization's personnel management practices, the organization should conduct a behavioral feasibility study before the imple- mentation phase-that is, in the analysis phase. The study should include an investigation ofthe levelsof employee acceptance of-and resistance to-change. Employees often feel threatened when an organization is creating or enhancing an information security program. Employees may perceive the program to bea manifestation of a Big Brother attitude, and mighth avequestions suchas:

- Why is management monitoring my work or my e-mail?
- Will information security staff go through my hard drive looking for evidence to fire me?
- How can I do my job well now that I have to deal with the added delays of the information security technology?

Resolving these sorts of doubts and reassuring employees about the role of information security programs are fundamental objectives of the implementation process. Thus, it is important to gather employee feedback early and respond to it quickly.

**Positioning and Staffing the Security Function**

There are several valid choices for positioning the information security department within an organization. The model commonly used by large organizations places the information security department within the information technology department and usually designates as its head the CISO (or CSO, Chief Security Officer), who reports directly to the company's top computing executive, or CIO. Such a structure implies that the goals and objectives of the CISO and CIO are aligned.

This is not always the case, however. By its very nature, aninformation security program can, at times, be at odds with the goals and objectives of the information technology department as a whole. The CIO, as the executive in charge of the organization's technology, strives to create efficiency in the processing and accessing of the organization's information, and thus, anything that limits access or slows information processing can impede the CIO's mission for the entire organization. The CISO's function is more like that of an internal auditor in that the CISO must direct the information security department to examine existing systems in order to discover information security faults and flaws in technology, software, and employees' activities and processes.

A good information security program maintains a careful balance between accessand security. Because the goals and objectives of CIOs and CISOs tend to contradict each other (in other words, the mission statements of the two functions conflict), the trend amongmany organizations has been to separate their information security function from their IT division. An article titled "Where the Chief Security Officer Belongs" published by the IT-industry magazine InformationWeek summarizes the reasoning behind this trend, perhaps as succinctly as possible: "the people who do and the people who watch shouldn't report to a common manager." A survey conducted by the consulting firm Meta Group found that while only 3 percent of its clients actually position the information security department outside IT, these clients regarded this positioning as the mark of a forward-thinking organization. Another group, Forrester Research, concludes that the traditional structure of the CISO/CSO reporting to the CIO structure will be prevalent for years to come, but that this structure will begin to involve numerous variations in which various IT sections report information to the CSO and thereby provide IS departments the critical input and control they need to protect the organization's IT assets.2In general, the data seems to suggest that while many organizations believe that the CISO/CSO should function as an independent, executive-level decision maker, infor- mation security and IT are currently too closely aligned to separate into two departments.

Information Security Roles and Responsibilities Made Easy, Charles CressonWood compiles many of the best practices regarding the positioning of information security programs from many industry groups.

- IT function, as a peer of other subfunctions such as networks, applications development, and the help desk
- Physical security function, as a peer of physical security or protective services Administrative services function, as a peer of human resources or purchasing Insurance and risk management function
- **Legal department**

  Once an information security function's organizational position has been determined, the challenge is to design a reporting structure that balances the competing needs of each of the com- munities of interest. The placement of the information security unit in the reporting structure often reflects the fact

that no one actually wants to manage it, and thus the unit is moved from place to place within the organization without regard to the impact on its effectiveness. Organizations should find a rational compromise by placing the information security function where it can best balance its duty to enforce organizational policy with its ability to provide the education, training, awareness, and customer service needed to make information security an integral part of the organizationalculture.

## 5.6 STAFFING THE INFORMATION SECURITY FUNCTION

**Q10. What are the certifications the information security personnel should aquire for fitting into their roles?**

*Ans :*

The selection of information security personnel is based on a number of criteria, some of which are within the control of the organization and some of which are not. Consider the fundamental concept of supply and demand. When the demand for any commodity-for example, a critical technical skill-increases too quickly, supply initially fails tomeet demand. Many future IS professionals seek to enter the security market by gaining the skills, experience, and credentials they need to meet this demand. In other words, they enter high- demand markets by changing jobs, going to school, or becoming trained. Until the new supply reaches the demand level, organizations must pay the higher costs associated withlimited supply. Once the supply meets or exceeds the demand, the organizations that are hiring people with these skills become selective, and the amount they are willing to pay drops. Hiring trends swing back and forth like a clock pendulum, from one end (high demand, low supply) to the other (low demand, high supply), because the real economy, unlike an econometric model, is seldom in a state of equilibrium. In 2002 the information security industry was in the midst of a period of high demand, with few qualified and experienced individuals available for organizations seeking their services.

But the latest forecasts for hiring in IT in general and information security in particular project more openings than in many previous years. According to the Bureau of Labor Statistics, information security positions and IT positions in general are predicted to continue to grow must faster than average for all occupations, with almost 300,000 new jobs expected over the 2008–2018 decade.3 According to a 2010 study, about 9 percent of CIOs are predicting being able to hire new IT (and InfoSec) professionals in the coming year, with information security being among the most difficult areas to hirefor.

### Qualifications and Requirements

A number of factors influence an organization's hiring decisions. Because information security has only recently emerged as a separate discipline, the hiring decisions in this field are further complicated by a lack of understanding among organizations about what qualifications a potential information security hire should exhibit. Currently in many organizations, information security teams lack established roles and responsibilities. Establishing better hiring practices in an organization requires the following:

- The general management community of interest should learn more about the skills and qualifications for both information security positions and those IT positions that impact informationsecurity.
- Upper management should learn more about the budgetary needs of the information security function and the positions within it. This will enable management to make sound fiscal decisions for both the information security function and the IT functions that carry out many of the information security initiatives.
- The IT and general management communities should grant appropriate levels of influence and prestige to the information security function, and especially to the role of chief information securityofficer.

In most cases, organizations look for a technically qualified information security generalist who has a solid understanding of how an organization operates. In many other fields, the more specialized professionals become, the more

marketable they are. In the information security discipline, however, overspecialization can be risky. It is important, therefore, to balance technical skills with general information security knowledge.

When hiring information security professionals, organizations frequently look for indivi- duals who understand thefollowing:

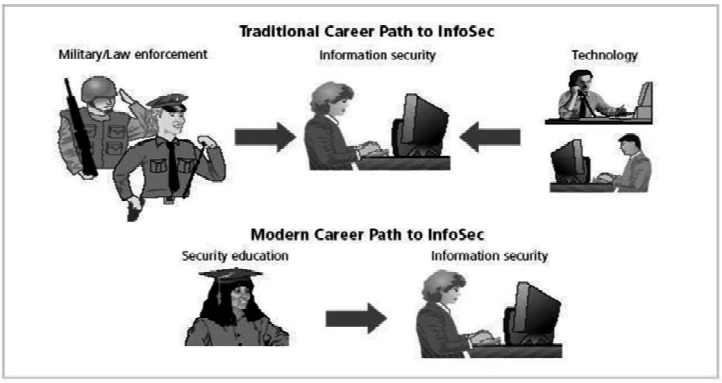
- How an organization operates at all levels That information security is usually a management problem and is seldom an exclusively technical problem
- How to work with people and collaborate with end users, and the importance of strong communications and writing skills
- The role of policy in guiding security efforts, and the role of education and training in making employees and other authorized users part of the solution, rather than part of the problem
- Most mainstream IT technologies (not necessarily as experts, but as generalists) The terminology of IT and information security
- The threats facing an organization and how these threats can become attacks How to protect an organization's assets from information security attacks
- How business solutions (including technology-based solutions) can be applied to solve specific information security problems

**Entry into the Information Security Profession**

Many information security professionals enter the field through one of two career paths: ex-law enforcement and military personnel involved in national security and cyber-security tasks, who move from those environments into business-oriented information security; and technical professionals - networking experts, programmers, database administrators, and systems administrators - who find themselves working on information security applications and processes more often than on traditional IT assignments. In recent years, a third (perhaps in some sense more traditional) career path has developed: college students who select and tailor their degree programs to prepare for work in the field of information security.

Many hiring managers in the information security field prefer to recruit security professionals who have proven IT skills and professional experience in another IT field. IT professionals who move into information security, however, tend to focus on technology—sometimes in place of general information security issues. Organizations can foster greater professionalism in the information security discipline by expanding beyond the hiring of proven IT professionals and instead filling positions by matching qualified candidates to clearly defined information security roles and positions

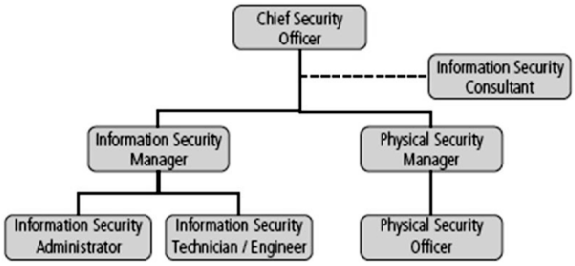
**Entering the Information Security Profession**



### Information Security Positions

The use of standard job descriptions can increase the degree of professionalism in the information security field as well as improve the consistency of roles and responsibilities among organizations. Organizations anticipating a revision of these roles and responsibilities can consult Charles Cresson Wood's book Information Security Roles and Responsibilities Made Easy, which offers a set of model job descriptions for information security positions. The chapteralso identifies the responsibilities and duties of the members of the IT staff whose work involves information security.

Definers provide the policies, guidelines and standards…They're the people who do the consulting and the risk assessment, who develop the product and technical architectures. These are senior people with alot of broad knowledge,but of ten not alot of depth … [Buildersare] there altechies, who create and installsecurity solutions…[Administrators] operate and administrate these curity tools [and] these curity monitoring function and … continuously improve the processes, per - forming all the day-to-day … work …. We often try to use the same people for all of these roles. We use builders all the time…. If you break your Info Sec profes - sionalsin to these three groups, you canrecruit the more efficiently, with the policy people being the more senior people, the builders being more technical and the operating people being those you cantraintodoa specific task.




**Chief Information Security Officer (CISO or CSO)** This is typically the top information security officer in the organization. As indicated earlier in the chapter, the CISO is usually not an executive-level position, and frequently the person in this role reports to the chief information officer. Though CISOs are business managers first and technologists second, they must be conversant in all areas of information security, including the technical, planning, and policy areas. In many cases, the CISO is the major definer or architect of the information security program. The CISO performs the following functions:

- Manages the overall information security program for the organization Drafts or approves information security policies
- Works with the CIO on strategic plans, develops tactical plans, and works with secu- rity managers on operational plans
- Develops information security budgets based on available funding
- Sets priorities for the purchase and implementation of information security projects and technology
- Makes decisions or recommendations on the recruiting, hiring, and firing of security staff
- Acts as the spokesperson for the information security team

The most common qualification for this type of position is the Certified Information Systems Security Professional (CISSP) accreditation. A graduate degree is also often required, although it may be from a number of possible disciplines, including information systems, computer science, another information technology field, criminal justice, military science, business, or other fields related to the broader topic of security. To qualify for this position, the candidate must demonstrate experience as a security manager, and present experience with planning, policy, and budgets. As mentioned earlier, some organizations prefer to hire individuals with law enforcement experience.

Security Manager Security managers are accountable for the day-to-day operation of the information security program. They accomplish objectives identified by the CISO and resolve issues identified by technicians. Management of technology requires an understanding of the technology administered, but does not necessarily require proficiency in the technology's configuration, operation, and fault resolution. (Note that there are a number of positions with titles that contain the word manager or other language that suggests management responsibilities, but only those people responsible for management functions, such as scheduling, setting relative priorities, or administering budgetary control, should be considered truemanagers.)

It is not uncommon for a candidate for this position to have a CISSP. Traditionally, managers earn the CISSP or CISM, and technical professionals earn the Global Information Assurance Certification (GIAC). Security managers must have the ability to draft middle- and lower-level policies as well as standards and guidelines. They must have experience in traditional business matters: budgeting, project management, hiring, and firing. They must also be able to manage technicians, both in the assignment of tasks and the monitoring of activities. Experience with business continuity planning is usually a plus. The following is an example of a typical security manager job description. Note that there are several different types of security managers, as the security manager position is much more specialized than that of CISO. Thus, when applying for a particular job, you should read that job's description carefully, as this is the best way to determine exactly what the employer is looking for.

The technical qualifications and position requirements for a security technician vary. Organizations prefer the expert, certified, proficient technician. Regardless of the area, the particular job description covers some level of experience with a particular hardware and software package. Sometimes familiarity with a technology secures an applicant an interview; how- ever, actual experience in using the technology is usually required.

## 5.7 Employment Policies and Practices

**Q11. What are the different practicies implemented for employment of a personnel**

*Ans :*

To create an environment in which information security is taken seriously, an organization should make information security a documented part of every employee's job description. In other words, the general management community of interest should integrate solid information security concepts into the organization's employment policies and practices. The section that follows examines the important information security-related issues associated with recruiting, hiring, firing, and managing human resources in anorganization.

From an information security perspective, the hiring of employees is a responsibility laden with potential security pitfalls. Therefore, the CISO and information security manager should establish a dialogue with the human resources department to provide information security input to the guidelines used for hiring all personnel.

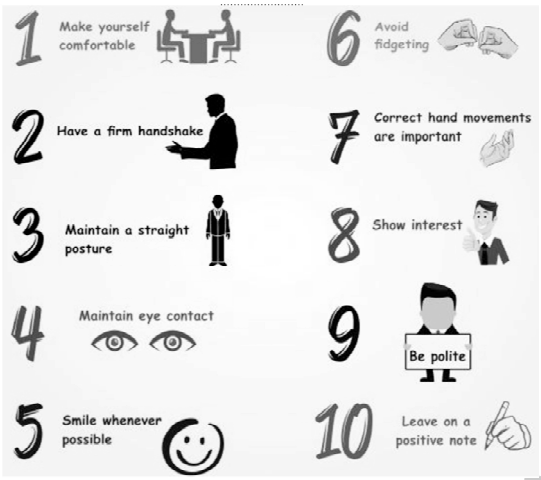
### Job Descriptions

The process of integrating information security perspectives into the hiring process begins with reviewing and updating all job descriptions. To prevent people from applying for positions based solely on access to sensitive information, the organization should avoid revealing access privileges to prospective employees when it advertises open positions.

### Interviews

Some interviews with job candidates are conducted with members of the human resources staff, and others include members of the department for which the new position is being offered. An opening within the information security department creates a unique opportunityfor the security manager to educate HR on the various certifications and the specific experience each certification requires, as well as the qualifications of a good candidate. In all other areas of the organization, information security should, for the same reason mentionedduringthe discussion of job

descriptions, advise HR to limit the information provided to the candidate about ther esponsibilities and accessrights that the new hire would have. For those organizations that include onsite visits as part of their initial or follow-up interviews, it is important to exercise caution when showing a candidate around the facility. Avoid tours through secure and restricted sites. Candidates who are shown around may be able to retain enough information about the operations or information security functions to become athreat.




**Background Checks**

A background check should be conducted before an organization extends an offer to a candidate. A background check is an investigation into the candidate's past that specifically looks forcriminal or other types of behavior that could indicate potential for future misconduct. There are a number of government regulations that govern what the organization can investigate and how much of the information uncovered can be allowed to influence the hiring decision. The security manager and HR manager should discuss these matters with legal counsel to determine what state and federal (and perhaps international) regulations impact the hiring process.

Background checks differ in the level of detail and depth with which they examine a candidate. In the military, background checks determine the individual's level of security classification, a requirement for many positions. In the business world, a background check can determine the level of trust the business places in the candidate. People being considered for security positions should expect to be subjected to a moderately high-level background check. Those considering careers in law enforcement or high-security positions may even be required to submit to polygraph tests. The following is a list of various types of background checks with the type of information each looksinto:

- **Identity checks:** Validation of identity and Social Security number
- **Education and credential checks:** Validation of institutions attended, degrees and certi- fications earned, and certification status.
- **Previous employment verification:** Validation of where candidates worked, why they left, what they did, and for how long.
- **Reference checks:** Validation of references and integrity of reference sources Worker's compensation history: Investigation of claims from worker's compensation .
- **Motor vehicle records:** Investigation of driving records,suspensi ons,andDUIs.
- **Drug history:** Screening for drugs and drug usage, past and present.
- **Credit history:** Investigation of credit problems, financial problems, and bank ruptcy.

- **Civil court history:** Investigation of involvement as the plaintiff or defendant in civil suits
- **Criminal court history:** Investigation of criminal background, arrests, convictions, and time served.

As mentioned, there are federal regulations regarding the use of personal information in employment practices, including the Fair Credit Reporting Act (FCRA), which governs the activities of consumer credit reporting agencies and the uses of theinformation procured from these agencies.

**Employment Contracts**

Once a candidate has accepted a job offer, the employment contract becomes an important security instrument. If an existing employee refuses to sign these contracts, the security per- sonnel are placed in a difficult situation. They may not be able to force the employee to sign nor to deny the employee access to the systems necessary to perform his or her duties. With new employees, however, security personnel are in a different situation since the procedural step of policy acknowledgment can be made a requirement of employment. Policies that govern employee behavior and are applied to all employees may be classified as "employment contingent upon agreement." This classification means the employee is not actually employed until he or she agrees in a written affidavit to conform withthese binding organizational policies. Some organizations choose to execute the remainder of the employment contract after the candidate has signed the security agreements. Although this may seem harsh, it is a neces- sarycomponent of the security process. Employment contracts may also contain restrictive clauses regarding the creation and ownership of intellectual property while the candidate is employed by the organization. These provisions may require the employee to protect the information assets of the organization actively- especially those assets that are critical to security.

**New Hire Orientation**

When new employees are introduced into the organization's culture and workflow, they should receive as part of their employee orientation an extensive information security briefing. All major policies should be explained, along with the procedures for performing neces- sary security operations and the new position's other information security requirements. In addition, the levels of authorized access should be outlined for the new employees, and train- ingshould be provided to them regarding the secure use of information systems. By the time new employees are ready to report to their positions, they should be thoroughly briefed on the security component of their particular jobs, as well as the rights and responsibilities of all personnel in the organization.

**On-the-Job Security Training**

The organization should integrate the security awareness education described into a new hire's ongoing job orientation and make it a part of every employee's on-the-job. securitytraining. Keeping security at the forefront of employees' minds helps minimize employee mistakes and is, therefore, an important part of the information security team's mission. Formal external and informal internal seminars should also be used to increase the security awareness level of employees, especially that of security employees.

**Evaluating Performance**

To heighten information security awareness and minimize workplace behavior that poses risks to information security, organizations should incorporate information security compo- nents into employee performance evaluations. For example, if employees have been observed writing system passwords on notes stuck to their monitor, they should be warned, and if such behavior continues, they should be reminded of their failure to comply with the organization's information security regulations during their annual performance review. In general, employees pay close attention to job performance evaluations and are more likely to be motivated to take information security seriously if their performance with respect to information security tasks and responsibilities is documented in theseevaluations.

**Termination**

Leaving the organization may or may not be a decision made by the employee. Organizations may downsize, be bought out or taken over, shut down, run out of business, or simply be forced to lay off, fire, or relocate their work force. In any

event, whenan employee leaves an organization, there are a number of security-related issues that arise. Key among these is the continuity of protection of all information to which the employee had access. Therefore, when anemployee prepares tole avean organization, the following tasks must be performed:

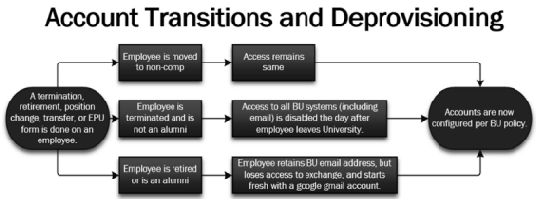
- Access to the organization's systems must be disabled.
- Removable media must be returned.
- Hard drives must be secured.
- File cabinet locks must be changed. Office door locks must be changed. Keycard access must be revoked.
- Personal effects must be removed from the organization's premises.

After the employee has delivered keys, keycards, and other business property, he or she should be escorted from the premises.

**Hostile departures** include termination for cause, permanent downsizing, temporary lay-off, or some instances of quitting. Before theemployee knows that he or she is leaving, or as soon as the hostile resignation is tendered, the security staff should terminate all logical and keycard access. In the case of involuntary terminations, the employee should be escorted into the supervisor's office for the bad news. Upon receiving the termination notice or tender- inga hostile resignation the employee should be escorted to his or her office, cubicle, or per- sonal area and allowed to collect personal effects. No organizational property should be allowed to be taken from the premises, including diskettes, pens, papers, and books. Regard- less of the claim the employee has on organizational property, he or she should not be allowed to take it from the premises. If there is property that theemployee strongly wishesto retain, the employee should be informed that he or she can submit, in writing, a list of the particular items and the reasons why he or she should be allowed to retain them. After the employee's personal property has been gathered, the employee should be asked to surren- der all company property such as (but not limited to) keys, keycards, organizational identifi- cation, physical access devices, PDAs, pagers, cell phones, and portable computers. The employee should then be escorted out of the building.

**Friendly departures** include resignation, retirement, promotion, or relocation. In this case, the employee may have tendered notice well in advance of the actual departure date. This sce- nario actually makes it much more difficult for the security team to maintain positive control over the employee's access and information usage. Employee accounts are usually allowed to continue to exist, though an expiration date can be set for the employee's declared date of departure. Another complication associated with friendly departures is that until their depar- turedate employees can come and go at will, which means they are usually collecting their own belongings and leaving under their own cognizance. As with hostile departures, employees should beasked to drop of fall organization alproperty on their final way out.

In either circumstance (hostile or friendly), the offices and information used by the employee must be inventoried, files must be stored or destroyed, and all property must be returned to organizational stores. It ispossible in either situation that the employees foresee their departure well in advance and, perhaps thinking that such items may be valuable in their future employment, start taking home organizational information such as files, reports, and data from data- bases. This may be impossible to prevent. Only by scrutinizing systems logs after the employee has departed and sorting out authorized actions from systems misuse or information theft can the organization determine if there has been a breach of policy or a loss of information. In the event that information is illegally copied or stolen, the action should be declared an incident and the appropriate policy followed.




## 5.8 CREDENTIALS FOR INFORMATION SECURITY PROFESSIONALS

**Q12. How the credentials of information security professionals are assessed?**

*Ans :*

Many organizations seek industry-recognized certifications to screen candidates for the required level of technical proficiency. Unfortunately, however, most of the existing certifications are relatively new andnot fully understood by hiring organizations. The certifying bodies are working hard to educate employers and potential professionalson the value and qualification soft heir certificate programs. In the meantime, employersare trying to understand the match between certifications and position requirements, and hopeful professionals are trying to gain meaningful employment based on their newly received certifications.

### (ISC)² Certifications

The International Information Systems Security Certification Consortium (ISC)2is considered one the foremost organizations offering information security certifications today. Currently (ISC)2 offers three primary certifications and three specializations for its flagship certification. (ISC)2 also offers an intermediate, or in-progress, certification to allow candidates who have not completed the experiential requirements of a certificationtoprovideevidenceofprogresstowardcompletingthecertification.

### Certified Information Systems Security Professional (CISSP)

In order to sit for the CISSP exam, the candidate must possess at least three years of direct full-time security professional work experience in one or more of the ten domains of information security knowledge listed below. The CISSP exam itself, which covers all ten domains, consists of 250multiple-choice questions and must be completed with in six hours.

- Access Control Application Security
- Business Continuity and Disaster Recovery Planning Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance, and Investigations Operations Security
- Physical (Environmental) Security Security Architecture and Design
- Telecommunications and Network Security

### CISSP Concentrations

In recent years, the CISSP certification program has added a set of concentration exams: the ISSEP (Information Systems Security Engineering Professional), the ISSAP (Information Systems Security Architecture Professional), and the ISSMP (Information Systems Security Management Professional). These certification extensions are designed to work in tandem with the CISSP credential; to sit for any of these concentration examinations, one must be a CISSP professional in good standing.

The development of the ISSEP concentration exam and its topical content are described by (ISC)2 as follows:

ISSEP stands for Information Systems Security Engineering Professional. ISSEP was developed under a joint agreement between (ISC)2 and the United States National Security Agency, Information Assurance Directorate (NSA/IAD). The motivation and justification for NSA's involvement in this project is found in NSD 42 and the Federal Technology Transfer Act of 1986 (15 U.S.C. Section 3710A).... The ISSEP provides the means for (ISC)2 to offer CISSPs a mechanism to demonst rate specific competence in the concentrated area of information security engineering.... The major domains of the ISSEP examination are: Systems Security Engineering, Certification and Accreditation, Technical Management, and U.S.Government In formation Assurance Regulations.

The development of the ISSAP concentration exam and its topical content are described by (ISC)2 as follows:

ISSAP stands for Information Systems Security Architecture Professional. The development of concentration examinations is a direct response to (ISC)2 research indicating that these needs of information security professionals were not being met. This examination is designed to provide CISSPs with a mechanism to demonstrate competence in the more in-depth and concentrated requirements of information security architecture, within the broader scope of information security knowledge identified in the CBK and required for CISSP certification. The major domains for this examination are: Access Control, Systems and Methodologies, Telecommunications and Network Security, Cryptography, Requirements Analysis &Security Standards, Guidelines, Criteria, and Technology Related BCP and DRP.

The development of the ISSMP concentration exam and its topical content are described by (ISC)2 as follows:

ISSMP stands for Information Systems Security Management Professional.The development of concentration examinations is a direct response to (ISC)2 research indicating that the seneeds of information security professionals were not being met. This examination is designed to provide CISSPs with a mechanism to demonstrate competence in the more in-depth and concentrated requirements of information security management.... The major domains for this examination are: Enterprise Security Management Practices, Enterprise- Wide System Development Security, Overseeing Compliance of Operations Security, Understanding BCP, DRP, and COOP, and Law, Investigations, Forensics, andEthics.

### Systems Security Certified Practitioner (SSCP)

Given the difficulty involved in mastering all ten domains, many information security professionals seek other, less rigorous certifications. In response, (ISC)2 developed the Systems Security Certified Practitioner, or SSCP. SSCP was designed to recognize mastery of an international standard for information security and a common body of knowledge (sometimes called the CBK). The SSCP certifica- tion is oriented toward the security administrator. Like the CISSP, the SSCP certification is more applicable to the information security manager than the technician, because most questions focus on the operational nature of information security. In other words, the SSCP focuses "on practices, roles, and responsibilities as defined by experts from major IS industries."15 Even so, an information security technician seeking advancement can benefit from acquiring this certification.

Instead of the tendomains of the CISSP, the SSCP coverssevendomains:

- Access Controls Cryptography
- Malicious Code and Activity
- Monitoring and Analysis Networks and Communications
- Risk, Response, and Recovery
- Security Operations and Administration

### Associate of (ISC)²

The Associate of (ISC)² program is geared toward those who want to take the CISSP or SSCP exams before obtaining the requisite experience for certification. "The Associate of (ISC)² program is a mechanism for information security professionals, who are still in the process of acquiring the necessary experience to become CISSPs or SSCPs, to become associated with (ISC)² and obtain career-related

support during this early period in his or her information security career."16 Once candidates pass the examination and subscribe to the (ISC)²Code of Ethics, they receive the Associate Certification indicating satisfactory progress toward a certification. Once the experiential requirements have been met, they receive their CISSP or SSCP.

**Certification and Accreditation Professional (CAP)**

The newest certification from (ISC)² is the Certification and Accreditation Professional (CAP), developedin cooperation with the U.S. Department of State's Office of Information Assurance. Certification and accreditation (C&A) was discussed in detail in Chapter 10. In order to qualify for the CAP certification, applicants must have a minimum of two years experience in one or more of the CAP common body of knowledged omainsand thus be prepared to:

- Initiate the preparation phase (formerly known as the certification and accreditation process and certification phase)
- Perform the execution phase (formerly known as the accreditation process)
- Perform the maintenance phase (formerly known as continuous monitoring)
- Understand the purpose of security authorization (formerly known as certification and accreditation, or C&A)

**ISACA Certifications**

The Information Systems Audit and Control Association (ISACA) was founded by a group of individuals with similar jobs in computer auditing who sought to provide a centralized source of information and guidance. Today ISACA offers two well-recognized and respected certifications: the CISA certification for auditing, networking, and security professionals, and the CISM certification for information security management professionals. All ISACA certifications have the following common requirements:

- Successful completion of the requisite examination
- Experience as an information systems auditor, with a minimum of five years' professional experience in an area of direct interest to the certification
- Agreement to the ISACA Code of Professional Ethics
- Continuing education policy that requires maintenance fees and a minimum of twenty contact hours of continuing education each year and a minimum of 120 contact hours over the three-year certification period

**Certified Information Systems Auditor (CISA)**

Although it does not primarily focus on information security certification, the Certified Information Systems Auditor or CISA certification covers many information security components. The CISA certification is open to those who have passed the CISA exam. The exam is offered once a year, contains 200 multiple-choice questions, and covers the following areas of information systems auditing:

- IS audit process (10 percent)-Provide IS audit services in accordance with IS audit standards, guidelines, and best practices to assist the organization in ensuring that its information technology and business systems are protected and controlled.
- IT governance (15 percent)-Provide assurance that the organization has the structure, policies, accountability, mechanisms, and monitoring practices in place to achieve the requirements of corporate governance of IT.
- Systems and infrastructure life cycle (16 percent)-Provide assurance that the management practices for the development/acquisition, testing, implementation, maintenance, and disposal of systems and infrastructure will meet the organization's objectives.
- IT service delivery and support (14 percent)-Provide assurance that the IT service management practices will ensure delivery of the level of services required to meet the organization's objectives.
- Protection of information assets (31 percent)-Provide assurance that the security architecture (policies, standards, procedures, and controls)

ensures the confidentiality, integrity, and availability of information assets.

- Business continuity and disaster recovery (14 percent)-Provide assurance that, in the event of a disruption, the business continuity and disaster recovery processes will ensure the timely resumption of IT services while minimizing the business impact.

**Certified Information Security Manager (CISM)**

The second ISACA certificate program is the CISM. This certificate is open to those who have passed the CISM require- ments, which are similar to the CISA. The applicant must pass the 200-question multiple- choice exam, which covers the following are as of information security practices:

- Information security governance (23 percent)
- Information risk management (22 percent)
- Information security program development (17percent)
- Information security program management (24 percent)
- Incident management and response (14 percent)

**SANS Global Information Assurance Certification(GIAC)**

The System Administration, Networking, and Security Organization, better known as SANS (www.sans.org), developed a series of technical security certifications in 1999 that are known as the Global Information Assurance Certification (GIAC) family of certifications (see www.giac.org). When the GIAC was established, no technical certificationswere avail- able elsewhere—anyone who wished to be certified to work in the technical security field could obtain only vendor-specific networking or computing certifications, such as the MCSE (Microsoft Certified Systems Engineer) or CNE (Certified Novell Engineer). Now, individuals canchoose to attain the various GIAC certifications separately or to pursue a comprehensive certification known as the GIAC Security Expert(GSE).

Unlike other certifications, the GIAC certifications require the applicant to complete a written practical assignment that tests the applicant's ability to apply skills and knowledge. These assignments are submitted to the SANS Information Security Reading Room for review by security practitioners, potential certificate applicants, and others with an interest in information security. Only when the practical assignment is complete is the candidate allowed to take the online exam. Once an individual has earned a particular GIAC certification, he or she can opt to earn an advanced recognition in that area by pursuing GIAC Gold Status for that certification by "completing a technical report covering an important area of security related to thecertification."

**Individual certifications include:**

- **Audit**
  - IAC Certified ISO-17799 Specialist (G7799)
  - GIAC Systems and Network Auditor (GSNA)
- **Legal**
  - GIAC Legal Issues (GLEG) Manage-ment
  - GIAC Information Security Professional (GISP) GIAC Security Leadership Certification (GSLC)
- GIAC Certified Project Manager Certification (GCPM) Security Administration
  - GIAC Information Security Fundame-ntals (GISF) GIAC Security Essentials Certification (GSEC)
  - GIAC Web Application Penetration Tester (GWAPT) GIAC Certified Forensic Analyst(GCFA)
  - GIAC Certified Enterprise Defender (GCED) GIAC Certified Firewall Analyst (GCFW) GIAC Certified Intrusion Analyst (GCIA) GIAC Certified Incident Handler(GCIH)
  - GIAC Certified Windows Security Administrator (GCWN) GIAC Certified UNIX Security Administrator (GCUX) GIAC Certified Penetration Tester (GPEN)
  - GIAC Reverse Engineering Malware (GREM) GIAC Assessing Wireless Networks (GAWN)

**Security Certified Program(SCP)**

One of the newer certifications in the information security discipline is the Security Certified Program's hands-on IT security certifications (see www.securitycertified.net). The SCP certifications provide three tracks: the SCNS (Security Certified Network Specialist), the SCNP (Security Certified Network Professional), and the SCNA (Security Certified Network Archi- tect). All three tracks are designed for the security technician and have dominant technical components, although the SCNA also emphasizes authentication principles. Also,eventhough the SCNS, SCNP, and SCNA each have a networking focus, they concentrate on network security rather than on true networking (which, for example, is covered by MSCE andCNE).

The SCNS track focuses on tactical perimeter defense with only one exam focused on its specialization:

| 20 Examination Domain | Percentage of Exam |
|---|---|
| 1.0 – Network Defense Fundamentals | 5% |
| 2.0 – Hardening Routers and Access Control Lists | 10% |
| 3.0 – Implementing IPSec and Virtual Private Networks | 10% |
| 4.0 – Advanced TCP/IP | 15% |
| 5.0 – Securing Wireless Networks | 15% |
| 6.0– Designing and Configuring Intrusion Detection Systems | 20% |
| 7.0 – Designing and Configuring Firewall Systems | 25% |

The SCNP track follows the SCNS exam and focuses on firewalls and intrusion detection. It requires one exam covering the following domains:

| Examination Domain | Percentage of Exam |
|---|---|
| 1.0 – Analyzing Packet Structures | 5% |
| 2.0 – Creating Security Policies | 5% |
| 3.0 – Performing Risk Analysis | 5% |
| 4.0 – Ethical Hacking Techniques | 10% |
| 5.0 – Internet and WWW Security | 15% |
| 6.0 – Cryptography | 20% |
| 7.0– Hardening Linux Computers | 20% |
| 8.0 – Hardening Windows Server 2003 | 20% |

The SCNA program follows the SCNP and focuses more on building trusted networks, including biometrics and PKI. The two exams in theSCNA certification are:

| Examination Domain | Percentage of Exam |
|---|---|
| 1.0 – Law and Legislation | 5% |
| 2.0 – Forensics | 15% |
| 3.0 – Wireless Security | 15% |
| 4.0 – Secure E-mail | 20% |
| 5.0 – Biometrics | 20% |
| 6.0 – PKI Policy and Architecture | 20% |
| 7.0 – Digital Certificates and Digital Signatures | 25% |
| 8.0 – Cryptography | 20% |
| 9.0 – Strong Authentication | 25% |

**Certified Computer Examiner (CCE)**

The Certified Computer Examiner (CCE)® certification is a computer forensics certification provided by the International Society of Forensic Computer Examiners (www.isfce.com). To complete the CCE certification process, the applicant must:

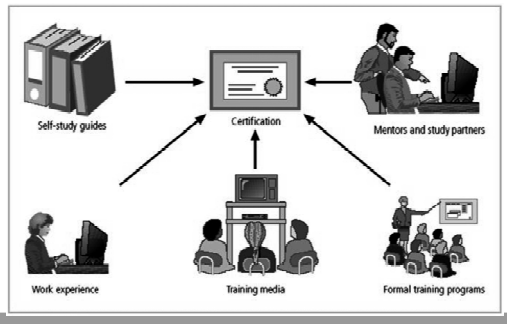
- Have no criminal record
- Meet minimum experience, training, or self-training requirements.
- Abide by the certification's code of ethical standards.
- Pass an online examination.
- Successfully perform actual forensic examinations on three test media.

**Certification Costs**

Certifications cost money, and the better certifications can be quite expensive to attain. Some certification exams can run as much as $650 per examination, and theirentire educational track can cost several thousand dollars. The cost of the formal training required to prepare for the certification can also be significant. While these courses should not serve as a candidate's only means of preparation, they can help round out knowledge and fill in gaps. As mentioned earlier, some of the exams, such as the CISSP, are very broad and others very technical. Even an experienced professional would find it difficult to sit for one of these exams without some preparation. Many candidates teach themselves using trade books. Others prefer the structure of classroom training, because it includes practicing the technical components on equipment the candidate may not be able to access on his or her own. Certifications are designed to recognize experts in their respective fields, and the cost of certification is meant to limit the number of candidates who take exams just to see if they can pass. Most examinations admit only candidates with two or three years of expertise in the skills being tested. Before attempting a certification exam, the successful candidate does all the required homework. Candidates for certification should look into the exam criteria, purpose, and requirements in order to ensure that the time and energy devoted to pursuing the certification are well spent.

**Advice for Information SecurityProfessionals**

- As a future information security professional, you may benefit from the following suggestions:
- Always remember: business before technology. Technology solutions are tools for solving business problems. Information security professionals are sometimes guilty of looking for ways to apply the newest technology to problems that do not require technology-based solutions
- When evaluating a problem, look at the source of the problem first, determine what factors impact the problem, and see where organizational policy can lead you in the design of a solution that is independent of technology; then use technology to deploy the controls necessary for the implementation of the solution. Technology can provide elegant solutions to some problems, but others it only exacerbates.
- That should be conducted from the security team to the users should be the periodic awareness messages, training announcements, newsletters, and e-mails.
- Know more than you say, and be more skillful than you let on. Don't try to impress users, managers, and other nontechnical people with your level of knowledge and experience. One day you just might run into a Jedi master of information security who puts you in yourplace.
- Speak to users, not at them. While you are talking to users, use their language, not yours. Users aren't Your job is to protect the organization's information and information systems resources.
- Never lose sight of the goal: protection. Be heard and not seen. Information security should be transparent to the users. With minor exceptions, the actions taken to protect the information should not interfere with the users' actions. Information security supports the work of end users, not the other way around. The only routine communications impressed with techno-babble and jargon. They may not comprehend the TLAs (three-letter acronyms), technical components, software, and hardware necessary to protect their systems, but they do know how to short-circuit your next budget request or pick out the flaws in your business report.




- Your education is never complete. As sensitive as you are to the fact that information technology is ever evolving, you must be equally sensitive to the fact that information security education is never complete. Just when you think you have mastered the latest skills, you will encounter changes in threats, protection technology, your business environment, or the regulatory environment. As a security professional, you must expect to continue with the learning process throughout your entire career. This is best accomplished by seeking out periodic seminars, training programs, and formal education. Even if the organization (or your pocketbook) cannot afford the more extensive and expensive training programs and conferences, you can keep abreast of the market by reading trade literature (magazines), textbooks, and news articles on security. You can also subscri be to the many mailing lists for information security professionals.
- Several are listed in the Offline entitled "What's in a Name?" Join at least one professional information security association, such as the Information Systems Security Association (www.issa.org). What ever approach you take, keep on top of there ading, nevers to plearning, and make yourself the best-informed security professional possible. It canonlyenhancey our worth to the organization and your career.

## 5.9 INFORMATION SECURITY MAINTENANCE

**Q13. How to select a security management maintance model?**

*Ans :*

To create or maintain a secure environment, one must design a working security plan and then implement a management model to execute and maintain the plan.

A framework is the outline of the more thorough blueprint, which is the basis for the design, selection, and implementation of all subsequent security controls.

To design a security blueprint, most organizations draw from established security models and practices.

**Security Management Models**

A security model is a generic blueprint offered by a service organization. One way to create the blueprint is to look at what other organizations have done (benchmarking).

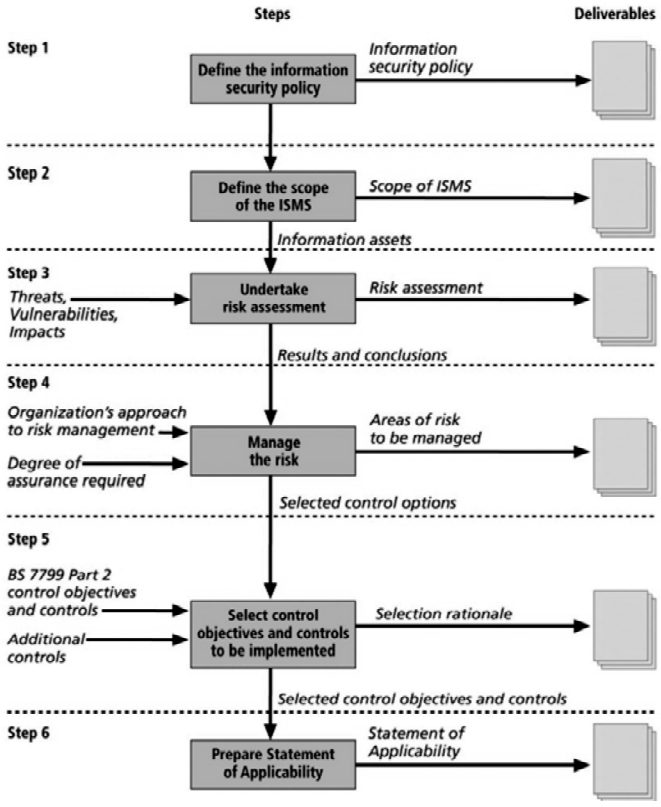
One way to select a methodology is to adapt or adopt an existing security management model or set of practices.

**BS 7799**

One of the most widely referenced and often discussed security models is Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799.

The purpose of ISO/IEC 17799 is to "give recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization.

It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings."



### ISO/IEC 17799 1 Drawbacks

1. The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
2. ISO/IEC 17799 lacks "the necessary measurement precision of a technical standard"
3. There is no reason to believe that ISO/IEC 17799 is more useful than any other approach
4. ISO/IEC 17799 is not as complete as other frameworks
5. ISO/IEC 17799 is perceived to have been hurriedly prepared, given the tremendous impact its adoption could have on industry information security controls

### The Ten Sections of ISO/IEC 17799

1. Organizational Security Policy is needed to provide management direction and support for information security.
2. Organizational Security Infrastructure objectives include:
   - Manage information security within the company
   - Maintain the security of organizational information processing facilities and information assets accessed by third parties
   - Maintain the security of information when the responsibility for information processing has been outsourced to another organization
3. Asset Classification and Control is needed to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.
4. Personnel Security objectives are:
   - Reduce risks of human error, theft, fraud or misuse of facilities
   - Ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work
   - Minimize the damage from security incidents and malfunctions and learn from such incidents
5. Physical and Environmental Security objectives include:
   - Prevent unauthorized access, damage and interference to business premises and information
   - Prevent loss, damage or compromise of assets and interruption to business activities
   - Prevent compromise or theft of information and information processing facilities
6. Communications and Operations Managem-ent objectives are:
   - Ensure the correct and secure operation of information processing facilities
   - Minimize the risk of systems failures
   - Protect the integrity of software and information
   - Maintain the integrity and availability of information processing and commun-ication
   - Ensure the safeguarding of information in networks and the protection of the supporting infrastructure
   - Prevent damage to assets and interruptions to business activities
   - Prevent loss, modification or misuse of information exchanged between organizations
1. System Access Control objectives in this area include:
   - Control access to information
   - Prevent unauthorized access to information systems
   - Ensure the protection of networked services

- Prevent unauthorized computer access
- Detect unauthorized activities
- Ensure information security when using mobile computing and telecommu-nication networks

2. System Development and Maintenance objectives include:
   - Ensure security is built into operational systems
   - Prevent loss, modification or misuse of user data in application systems
   - Protect the confidentiality, authenticity and integrity of information.
   - Ensure IT projects and support activities are conducted in a secure manner
   - Maintain the security of application system software and data
3. Business Continuity Planning to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.
4. Compliance objectives include:
   - Avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
   - Ensure compliance of systems with organizational security policies and standards
   - Maximize the effectiveness of and minimize interference to/from the system audit process BS 7799 provides implementation details using a Plan-Do-Check-Act cycle.

### The Security Management Index and ISO 17799

One way to determine how closely an organization is complying with ISO 17799 is to take the Human Firewall Council's survey, the Security Management Index (SMI).

The SMI asks 35 questions over the 10 domains of the ISO standard.

"This survey gathers metrics on how organizations manage security and enables information security officers to benchmark their practices against those of other organizations. The survey has been developed according to ISO 17799 international security standards to reflect best practices from a global perspective. The Security Management Index survey will help you measure your security management practices compared to other organizations in your industry and peer group."

The Human Firewall Council recommends:

- Familiarize yourself with the 10 categories of security management.
- Benchmark your organization's security management practices by taking the survey.
- Evaluate your results in each category to identify strengths and weaknesses.
- Examine the suggestions for improvement in each category in this report.
- Use your SMI results to gain support for improving security.

### RFC 2196 Site Security Handbook

The Security Area Working Group within the IETF has created RFC 2196.The Security Area Working Group acts as an advisory board for the protocols and areas developed and promoted through the Internet Society.

**RFC 2196:** Site Security Handbook does provide a good functional discussion of important security issues and provides an overview of five basic areas of security, along with development and implementation details.

There are chapters on such important topics as security policies, security technical architecture, security services, and security incident handling.

The architecture begins with a discussion of the importance of security policies, and expands into an examination of services, access controls, and other relevant areas.

### NIST Security Models

NIST documents have two notable advantages:

They are publicly available at no charge; and they have been available for some time and thus have been broadly reviewed by government and industry professionals.

- SP 800-12, Computer Security Handbook
- SP 800-14, Generally Accepted Security Principles & Practices
- SP 800-18, Guide for Developing Security Plans
- SP 800-26, Security Self-Assessment Guide-IT Systems
- SP 800-30, Risk Management for Information Technology Systems

### NIST SP 800-12

SP 800-12 is entitled The Computer Security Handbook, and is an excellent reference and guide for the routine management of information security.

It provides little guidance, however, on design and implementation of new security systems; use it as a supplement to gain a deeper understanding in the background and terminology.

800-12 also lays out the NIST philosophy on security management by identifying 17 controls organized into three categories:

- The Management Controls section addresses security topics that can be characterized as managerial.
- The Operational Controls section addresses security controls that focus on controls that are, broadly speaking, implemented and executed by people (as opposed to systems).
- The Technical Controls section focuses on security controls that the computer system executes.

### NIST Special Publication 800-14

NIST SP800-14, subtitled Generally Accepted Principles and Practices for Securing Information Technology Systems, describes best practices and provides information on commonly accepted information security principles that can direct the security team in the development of a security blueprint.

It also describes the philosophical principles that the security team should integrate into the entire information security process, expanding upon the components of SP 800-12.

The more significant points made in NIST SP 800-14 are as follows:

1. Security Supports the Mission of the Organization.
2. Security is an Integral Element of Sound Management.
3. Security Should Be Cost-Effective
4. Systems Owners Have Security Responsibilities Outside Their Own Organizations.
5. Security Responsibilities and Accountability Should Be Made Explicit.
6. Security Requires a Comprehensive and Integrated Approach.
7. Security Should Be Periodically Reassessed.
8. Security is constrained by Societal Factors.

It enumerates 33 principles for Securing Information Technology Systems:

- **Principle 1-** Establish a sound security policy as the "foundation" for design.
- **Principle 2-** Treat security as an integral part of the overall system design.
- **Principle 3-** Clearly delineate the physical and logical security boundaries governed by associated security policies.
- **Principle 4-** Reduce risk to an acceptable level.
- **Principle 5-** Assume that external systems are insecure.
- **Principle 6-** Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
- **Principle 7-** Implement layered security (Ensure no single point of vulnerability).
- **Principle 8-** Implement tailored system security measures to meet organizational security goals.
- **Principle 9-**Strive for simplicity.
- **Principle 10-** Design and operate an IT system to limit vulnerability and to be resilient in response.
- **Principle 11-** Minimize the system elements to be trusted.
- **Principle 12-** Implement security through a combination of measures distributed physically and logically.
- **Principle 13-** Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
- **Principle 14-** Limit or contain vulnerabilities.
- **Principle 15-** Formulate security measures to address multiple overlapping information domains.
- **Principle 16-** Isolate public access systems from mission critical resources.
- **Principle 17-** Use boundary mechanisms to separate computing systems and network infrastructures.
- **Principle 18-** Where possible, base security on open standards for portability and interoperability.
- **Principle 19-** Use common language in developing security requirements.
- **Principle 20-** Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
- **Principle 21-** Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.

- **Principle 22-** Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
- **Principle 23-** Use unique identities to ensure accountability.
- **Principle 24-** Implement least privilege.
- **Principle 25-** Do not implement unnecessary security mechanisms.
- **Principle 26-**Protect information while being processed, in transit, and in storage.
- **Principle 27-** Strive for operational ease of use.
- **Principle 28-** Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
- **Principle 29-** Consider custom products to achieve adequate security.
- **Principle 30-** Ensure proper security in the shutdown or disposal of a system.
- **Principle 31-** Protect against all likely classes of "attacks."
- **Principle 32-** Identify and prevent common errors and vulnerabilities.
- **Principle 33-** Ensure that developers are trained in how to develop secure software.

### NIST Special Publication 800-18

NIST SP 800-18 - A Guide for Developing Security Plans for Information Technology Systems, provides detailed methods for assessing, designing, and implementing controls and plans for various sized applications.

SP 800-18 serves as a guide for the activities described in this chapter, and for the overall information security planning process.

It includes templates for major application security plans.

### NIST Special Publication 800-26

NIST SP 800-26 - Security Self-Assessment Guide for Information Technology Systems describes seventeen areas that span managerial, operational and technical controls. The 17 areas listed are the core of the NIST security management structure.

### NIST Special Publication 800-30

NIST SP 800-30 - Risk Management Guide for Information Technology Systems provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems.

The ultimate goal is to help organizations to better manage IT-related mission risks.

### Security Management Practices

- In information security, two categories of benchmarks are used: standards of due care/ due diligence, and best practices.
- Best practices include a sub-category of practices—called the gold standard—that are general regarded as "the best of the best."

### Standards of Due Care/Due Diligence

- When organizations adopt minimum levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances; this is known as a standard of due care.
- Implementing controls at this minimum standard, and maintaining them, demonstrates that an organization has performed due diligence.

  Due diligence requires that an organization ensure that the implemented standards continue to provide the required level of protection.

  Failure to support a standard of due care or due diligence can expose an organization to legal liability, provided it can be shown that the organization was negligent in its application or lack of application of information protection.

### Best Security Practices

Security efforts that seek to provide a superior level of performance in the protection of information

are referred to as best business practices or simply best practices.Some organizations refer to these as recommended practices.

Security efforts that are among the best in the industry are referred to as best security practices

These practices balance the need for information access with the need for adequate protection. Best practices seek to provide as much security as possible for information and information systems while demonstrating fiscal responsibility and ensuring information access.

Companies with best practices may not be the best in every area; they may only have established an extremely high quality or successful security effort in one area.

### VISA International Security Model

Another example of best practices is the VISA International Security Model.

VISA has developed two important documents that improve and regulate its information systems:

- The "Security Assessment Process" document contains a series of recommendations for the detailed examination of an organization's systems with the eventual goal of integration into the VISA systems.
- The "Agreed upon Procedures" document outlines the policies and technologies used to safeguard security systems that carry the sensitive cardholder information to and from VISA systems.

### The Gold Standard

Best business practices are not sufficient for organizations that prefer to set the standard by implementing the most protective, supportive, and yet fiscally responsible standards they can. They strive toward the gold standard, a model level of performance that demonstrates industrial leadership, quality, and concern for the protection of information.

- The implementation of gold standard security requires a great deal of support, both in financial and personnel resources.

### Selecting Best Practices

- Choosing which recommended practices to implement can pose a challenge for some organizations.
- In industries that are regulated by governmental agencies, government guidelines are often requirements.
- For other organizations, government guidelines are excellent sources of information about what other organizations are required to do to control information security risks, and can inform their selection of best practices.

### Selecting Best Practices

When considering best practices for your organization, consider the following :

- Does your organization resemble the identified target organization of the best practice?
- Are you in a similar industry as the target?
- Do you face similar challenges as the target?
- Is your organizational structure similar to the target?
- Are the resources you can expend similar to those called for by the best practice?
- Are you in a similar threat environment as the one assumed by the best practice?

Microsoft has published a set of best practices in security at its Web site :

- Use antivirus software
- Use strong passwords
- Verify your software security settings
- Update product security
- Build personal firewalls
- Back up early and often
- Protect against power surges and loss

### Benchmarking and Best Practices Limitations

The biggest problem with benchmarking in information security is that organizations don't talk

to each other; a successful attack is viewed as an organizational failure, and is kept secret, insofar as possible.

However, more and more security administrators are joining professional associations and societies like ISSA and sharing their stories and lessons learned. An alternative to this direct dialogue is the publication of lessons learned.

**Baselining**

- A baseline is a "value or profile of a performance metric against which changes in the performance metric can be usefully compared."
- Baselining is the process of measuring against established standards. In InfoSec, baselining is the comparison of security activities and events against the organization's future performance.
- Baselining can provide the foundation for internal benchmarking, as information gathered for an organization's first risk assessment becomes the baseline for future comparisons.
- The Gartner group offers twelve questions as a self assessment for best security practices.

**People**

1. "Do you perform background checks on all employees with access to sensitive data, areas, or access points?
2. "Would the average employee recognize a security issue?
3. "Would they choose to report it?
4. "Would they know how to report it to the right people?

**Processes**

1. "Are enterprise security policies updated on at least an annual basis, employees educated on changes, and consistently enforced?
1. "Does your enterprise follow a patch/update management and evaluation process to prioritize and mediate new security vulnerabilities?
2. "Are the user accounts of former employees immediately removed on termination?
3. "Are security group representatives involved in all stages of the project life cycle for new projects?

**BaseliningTechnology**

1. "Is every possible route to the Internet protected by a properly configured firewall?
2. "Is sensitive data on laptops and remote systems encrypted?
3. "Do you regularly scan your systems and networks, using a vulnerability analysis tool, for security exposures?
4. "Are malicious software scanning tools deployed on all workstations and servers?"

**Q14. Explain & list different certifications and accredation in initiative way to secure you data standards?**

*Ans :*

In security management, accreditation is the authorization of an IT system to process, store, or transmit information.

It is issued by a management official and serves as a means of assuring that systems are of adequate quality.

It also challenges managers and technical staff to find the best methods to assure security, given technical constraints, operational constraints, and mission requirements.

Certification is "the comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements."

Organizations pursue accreditation or certification to gain a competitive advantage, or to provide assurance or confidence to customers.

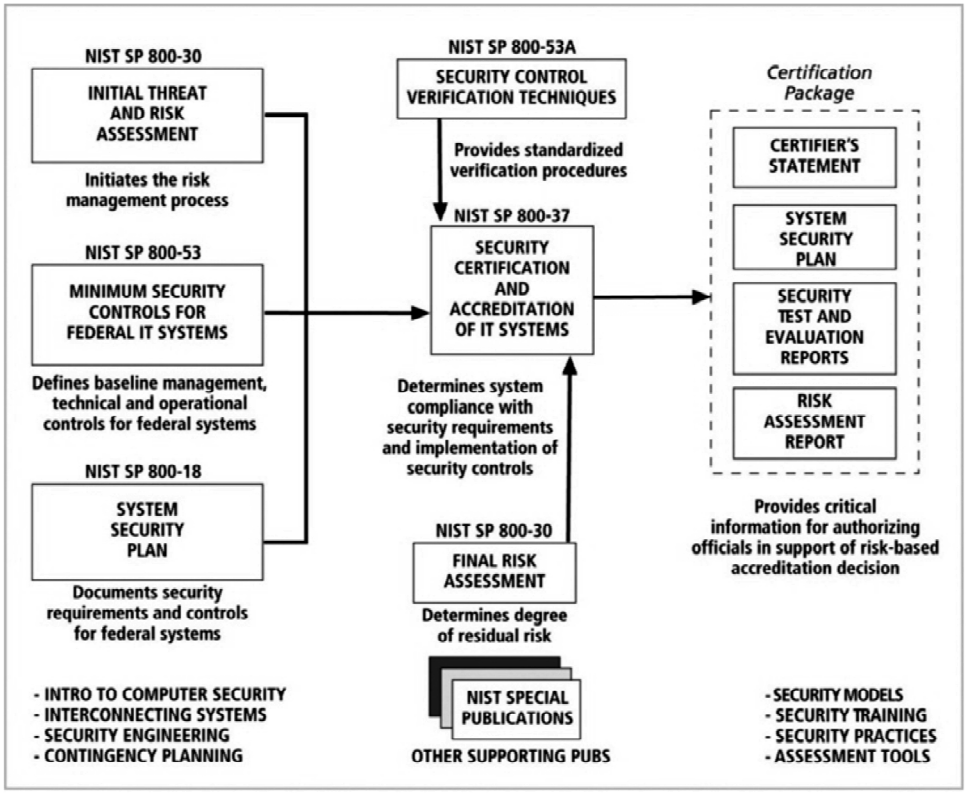
**SP 800-37**

Guidelines for the Security Certification and Accreditation of Federal IT systems. NIST promotes a new System Certification and Accreditation Project designed to:

- Develop standard guidelines and procedures for certifying and accrediting federal IT systems including the critical infrastructure of the United States
- Define essential minimum security controls for federal IT systems
- Promote the development of public and private sector assessment organizations and certification of individuals capable of providing cost effective, high quality, security certifications based on standard guidelines and procedures

The specific benefits of the security certification and accreditation (C&A) initiative include :

- More consistent, comparable, and repeatable certifications of IT systems
- More complete, reliable, information for authorizing officials—leading to better understanding of complex IT systems and associated risks and vulnerabilities—and therefore, more informed decisions by management officials
- Greater availability of competent security evaluation and assessment services
- More secure IT systems within the federal government"
- This project is also designed to promote development of:
- A standardized process for certifying and accrediting Federal information systems including the critical infrastructure of the United States
- Minimum security controls for Federal information and IS supporting confidentiality, integrity, and availability
- Techniques and procedures for verifying the effectiveness of security controls for Federal IS
- Robust, automated tools supporting the certification and accreditation process
- Public and private sector assessment organizations capable of providing cost effective, high quality, certification services

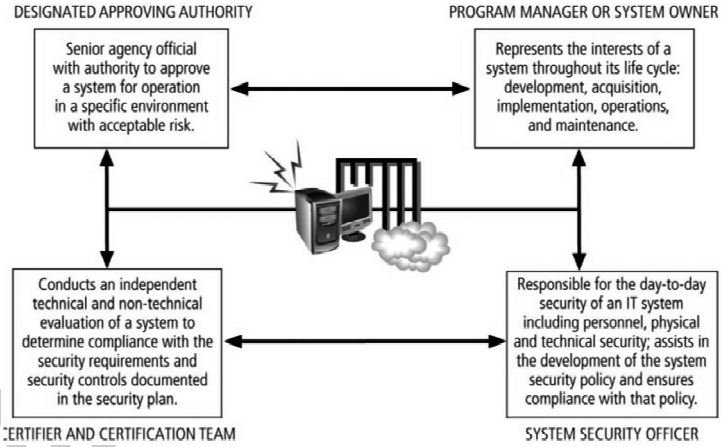


**800-37 focuses on a three-step security controls selection process:**

- **Step 1:** Characterize the System
- **Step 2:** Select the Appropriate Minimum Security Controls for the System
- **Step 3:** Adjust Security Controls Based On System Exposure and Risk Decision

**Systems Are Certified To One of Three Levels**

- **"Security Certification Level 1 -** The Entry-Level Certification Appropriate For Low Priority (Concern) Systems.
- **"Security Certification Level 2 -** The Mid-Level Certification Appropriate For Moderate Priority (Concern) Systems.
- **"Security Certification Level 3 -** The Top-Level Certification Appropriate For High Priority (Concern) Systems.




SP 800-53 - Minimum Security Controls for Federal IT Systems

- SP 800-53 is part two of the Certification and Accreditation project.
- Its purpose is to "establish a set of standardized, minimum security controls for IT systems addressing low, moderate, and high levels of concern for confidentiality, integrity, and availability."
- As in earlier NIST documents, especially SP 800-18, security controls are broken into the three familiar general classes of security controls - management, operational, and technical.
- New to the certification and accreditation criteria is the concept of critical elements, initially defined in SP 800-26.
- Critical elements represent "important security-related focus areas for the system with each critical element addressed by one or more security controls."
- As technology evolves so will the set of security controls, requiring additional control mechanisms.

# FACULTY OF INFORMATICS

**M.C.A III Year I - Semester Examination**

**MODEL PAPER - I**

## INFORMATION SECURITY

**Time : 3 Hours]** **[Max. Marks : 70**

**Answer all the question according to the internal choice**

**(5 × 14 = 70 Marks)**

1. (a) List and explain the critical characteri-stics of information security? **(Unit -I, Q.No.2)**

   (b) What are the 3 components C.I.A traingle? What are they used for? Why is it so commonly use in security? **(Unit -I, Q.No.9)**

   **OR**

   (c) Explain different stages of development in SDLC. **(Unit -I, Q.No.7)**

2. (a) What is Risk management? State the methods of identifying & assessing risk management? **(Unit -II, Q.No.6)**

   (b) Explain in detail different Risk control strategies? **(Unit -II, Q.No.11)**

   **OR**

   (c) What are the different ocuments of requirements to solving Risk Management? **(Unit -II, Q.No.14)**

3. (a) Explain with diagram the design of Security Architecture? **(Unit -III, Q.No.6)**

   (b) What are wall rule? Explain different firewall rules sets? **(Unit -III, Q.No.13)**

   **OR**

   (c) Write a short notes on (a) Screened subnet fire walls (DMZ) (b) Screened host fire wall. **(Unit -III, Q.No.11)**

4. (a) What are the different types of intrusion detection system avaliable? Explain with read diagram? **(Unit -IV, Q.No.2)**

   (b) What are the purposes of scanning and analysis tools? Who will be using these tools? **(Unit -IV, Q.No.6)**

   **OR**

   (c) Explain different cryptographic algori-thms in detail? **(Unit -IV, Q.No.14)**

5. (a) Explain in detail the Bull's-eye model in solving systematic & measure way of information security? **(Unit -V, Q.No.4)**

   (b) What are the 4 phases of NIACAP & instructions? What NIACAP certification levels are recommeded by the security levels? **(Unit -V, Q.No.7)**

   **OR**

   (c) Explain & list different certifications and accrediation in initiative way to secure you data standards? **(Unit -V, Q.No.14)**

# FACULTY OF INFORMATICS

**M.C.A III Year I - Semester Examination**

**MODEL PAPER - II**

## INFORMATION SECURITY

**Time : 3 Hours]** **[Max. Marks : 70**

**Answer all the question according to the internal choice**

**(5 × 14 = 70 Marks)**

1. (a) What are the different stages of security SDLC in detail? **(Unit -I, Q.No.8)**

   (b) What are threats? Explain different categories of threats? **(Unit -I, Q.No.10)**

   **OR**

   (c) Explain the principles & Development of Sec Development life cycle of software. **(Unit -I, Q.No.12)**

2. (a) Explain in detail the legal, ethical & professional issues during the security investigation? **(Unit -II, Q.No.4)**

   (b) Explain asset identification & valuation of Risk? **(Unit -II, Q.No.8)**

   **OR**

   (c) Explain in detail the process of asset identification of different Strategies of selecting & Controling Risk? **(Unit -II, Q.No.12)**

3. (a) What are ISO17799 and BS 7799? Explain different sections & Sailent features? **(Unit -III, Q.No.2)**

   (b) Explain in detail different firewall architectures? **(Unit -III, Q.No.9)**

   **OR**

   (c) Write a short notes on (a) Dial-Up (b) RADIUS and TACACS (c) Kerberos security **(Unit -III, Q.No.15)**

4. (a) Write a short notes deployment and accers of ne/w on IDS (a) Network base IDS (b) Hotspot base IDS (c) Application base IDS **(Unit -IV, Q.No.4)**

   (b) List few crypto system principles? **(Unit -IV, Q.No.11)**

   **OR**

   (c) What is RSA algorithm? Explain different steps? **(Unit -IV, Q.No.15)**

5. (a) What are certifications that information security personnely should aquire? **(Unit -V, Q.No.6)**

   **OR**

   (b) What are the different practicies implemented for employment of a personnel **(Unit -V, Q.No.11)**

# FACULTY OF INFORMATICS

**M.C.A III Year I - Semester Examination**

**MODEL PAPER - III**

## INFORMATION SECURITY

**Time : 3 Hours]** **[Max. Marks : 70**

**Answer all the question according to the internal choice**

**(5 × 14 = 70 Marks)**

1. (a) Explain the 2 functional approaches of information security performed by organization. **(Unit -I, Q.No.5)**
   (b) Explain the best planning & implementation of Information Security. **(Unit -I, Q.No.6)**

**OR**

   (c) What are the different stages of security SDLC in detail? **(Unit -I, Q.No.8)**
2. (a) What are international laws on laws & legal bodies? **(Unit -II, Q.No.3)**
   (b) What is risk management? What is the identification of risk by listing assets & vulnerabilities is so important in the risk management process? **(Unit -II, Q.No.9)**

**OR**

   (c) Explain the relation b/w Qualitative & Quantative Analysis of Risk Management? **(Unit -II, Q.No.13)**
3. (a) What is information security Blue Print? Explain its sailent features. **(Unit -III, Q.No.5)**
   (b) What are the factors to be considered in selecting a right fire wall? Outline some of the best practicies firewall use? **(Unit -III, Q.No.12)**

**OR**

   (c) Explain in detail firewalls categorized by processing model different generation of firewalls? **(Unit -III, Q.No.10)**
4. (a) What is intrusion detection system? Explain different reasons and terminology associated. **(Unit -IV, Q.No.1)**
   (b) What is the purpose of firewall analysis tools? Why? **(Unit -IV, Q.No.7)**

**OR**

   (c) What are the different possible attacks on crypto system? Explain with either methods. **(Unit -IV, Q.No.12)**
5. (a) Explain the need of project plan? **(Unit -V, Q.No.2)**
   (b) What is 27001/27002? What are the benefits of ISO 27001/27002? What is the cost of cetification? **(Unit -V, Q.No.8)**

**OR**

   (c) How the credentials of information security professionals are assessed? **(Unit -V, Q.No.12)**
   (d) How to select a security management maintance model? **(Unit -V, Q.No.13)**